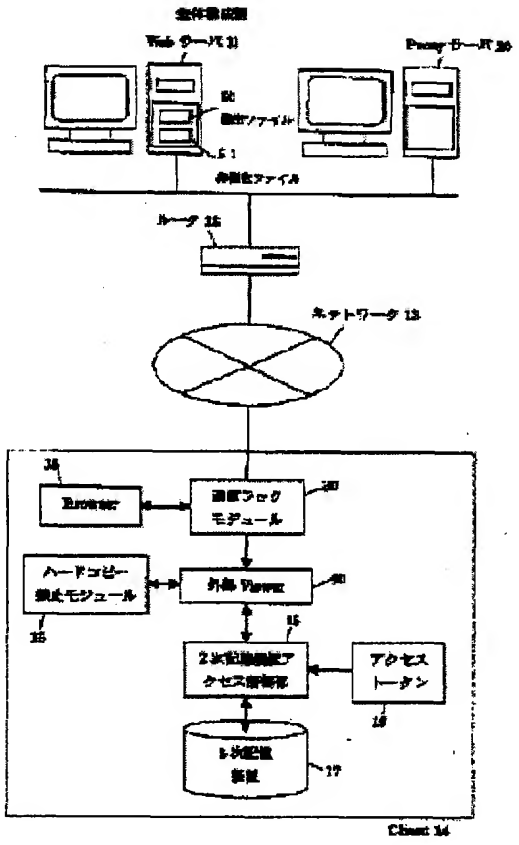
INFORMATION PRESENTATION SYSTEM AND DEVICE

Publication number: JP2002041347
Publication date: 2002-02-08
Inventor: KIRIHATA YASUHIRO
Applicant: HITACHI SOFTWARE ENG
Classification:
- International: ***G06F12/14; G06F12/00; G06F15/00; G06F21/20; G06F21/24; G09C1/00;*** **G06F12/14; G06F12/00; G06F15/00; G06F21/00; G06F21/20; G09C1/00;** (IPC1-7): G06F12/00; G06F12/14; G06F15/00
- European:
Application number: JP20010062780 20010307
Priority number(s): JP20010062780 20010307; JP20000144304 20000517

Report a data error here

Abstract of **JP2002041347**

PROBLEM TO BE SOLVED: To enable only a person having an access right via a network to browse confidential information in a data base constructed on the existing Web server similar to a general page without altering the existing Web server and without depending on hardware structure of a device such as a client computer at a requesting origin. SOLUTION: This system is provided with a repeater to accept a transfer request from the device at the requesting origin to presentation object data held by a computer via the network, to authenticate the access right of the device at the requesting origin itself or a user at the requesting origin, to acquire the presentation object data from the computer according to the result of the authentication and to transfer the data to the device at the requesting origin.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－41347
（P2002－41347A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.[7]		識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ａ　５Ｂ０１７
		５４６			５４６Ｔ　５Ｂ０８２
	12/14	３２０		12/14	３２０Ｂ　５Ｂ０８５
					３２０Ａ
	15/00	３３０		15/00	３３０Ｄ

審査請求　未請求　請求項の数27　ＯＬ　（全 40 頁）

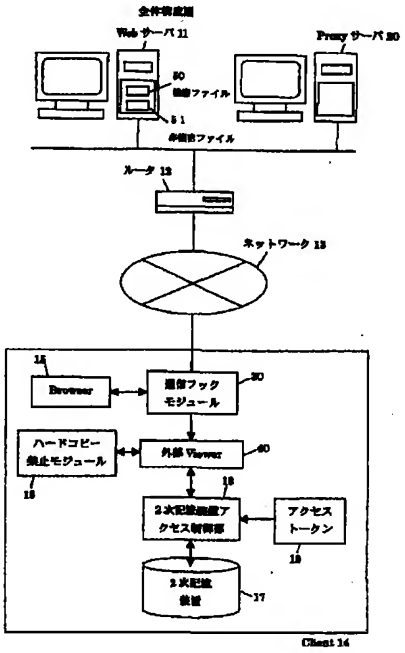
(21)出願番号　特願2001－62780(P2001－62780)
(22)出願日　平成13年３月７日(2001.3.7)
(31)優先権主張番号　特願2000－144304(P2000－144304)
(32)優先日　平成12年５月17日(2000.5.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　桐畑　康裕
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100088720
弁理士　小川　眞一

Ｆターム(参考)　5B017 AA07 BA06 CA16
5B082 EA11 GB02
5B085 AE06 BG07

(54)【発明の名称】　情報提供システムおよび装置

(57)【要約】
【課題】　既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能にすること。
【解決手段】　ネットワークを介してコンピュータが保持している提供対象データに対する要求元装置からの転送要求を受付け、当該要求元装置自身または要求元ユーザのアクセス権限の認証を行い、その認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する中継装置を備える。



1

【特許請求の範囲】

【請求項１】　コンピュータが保持している提供対象のデータをネットワークを介して要求元装置に転送する情報提供システムであって、

ネットワークを介して前記コンピュータが保持している提供対象データに対する要求元装置からの転送要求を受付け、当該要求元装置自身または要求元ユーザのアクセス権限の認証を行い、その認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する中継装置を備えることを特徴とする情報提供システム。

【請求項２】　前記コンピュータはアクセス権限の認証を必要とする第１の提供対象データと、認証を必要としない第２の提供対象データとを保持するものであり、

前記中継装置は前記第１の提供対象データに対する転送要求受付け時にアクセス権限の認証を行なうことを特徴とする請求項１記載の情報提供システム。

【請求項３】　前記中継装置は、要求元装置に転送する第１の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする請求項２記載の情報提供システム。

【請求項４】　前記要求元装置は、前記中継装置から受信した暗号化された第１の提供対象データを自装置または要求元ユーザに固有の暗号鍵に対応した復号鍵で復号する復号処理手段と、復号された第１の提供対象データを出力する第１の出力手段と、中継装置から受信した前記第２の提供対象データを出力する第２の出力手段を備えることを特徴とする請求項３記載の情報提供システム。

【請求項５】　前記要求元装置は、前記中継装置から受信したデータに付加されている識別子により第１の提供対象データであるか、第２の提供対象データであるかを判定し、第１の提供対象データである場合に前記第１の出力手段を起動する手段と、第１の出力手段が正常に起動できなければ中継装置から受信した第１の提供対象データを削除する手段とを備えることを特徴とする請求項４記載の情報提供システム。

【請求項６】　前記要求元装置は、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第１の提供対象データを暗号化して２次記憶装置に保管する手段とを備えることを特徴とする請求項４または５記載の情報提供システム。

【請求項７】　前記要求元装置は、前記第１の出力手段に出力された第１の提供対象データのハードコピーを禁止する手段を備えることを特徴とする請求項４～６のいずれか一項に記載の情報提供システム。

【請求項８】　前記要求元装置は、要求元装置内のアプリケーションから前記２次記憶装置への入出力を監視

2

し、前記第１の出力手段を介在しない第１の提供対象データに対するアクセスを禁止する２次記憶アクセス制御手段とを備えることを特徴とする請求項７記載の情報提供システム。

【請求項９】　前記要求元装置は、前記ハードコピーを禁止する手段及び前記２次記憶アクセス制御手段が共に正常に動作していない限り前記第１の出力手段を起動させない手段を備えることを特徴とする請求項８記載の情報提供システム。

【請求項１０】　前記中継装置および要求元装置は、要求元装置のユーザのアクセス権限の認証を行なうためのアクセス権限判定用情報を記憶した第１の記憶手段をそれぞれ備えることを特徴とする請求項６記載の情報提供システム。

【請求項１１】　前記要求元装置は、前記２次記憶装置に保管された第１の提供対象データへのアクセスの都度または所定の時期に、前記中継装置内の前記第１の記憶手段に記憶されたアクセス権限判定用情報を取得し、自装置内の第１の記憶手段に記憶されているアクセス権限判定用情報を最新バージョンに更新する手段とを備え、更新されたアクセス権限判定用情報により、前記２次記憶装置に保管された第１の提供対象データへのアクセス権限の有無を判定することを特徴とする請求項１０記載の情報提供システム。

【請求項１２】　前記中継装置は、要求元装置からの転送要求に付加されている要求元装置識別情報によってアクセス権限の認証を行なうことを特徴とする請求項１～９のいずれか一項に記載の情報提供システム。

【請求項１３】　前記中継装置は、要求元装置からユーザ識別情報を取得してアクセス権限の認証を行なうことを特徴とする請求項１～９のいずれか一項に記載の情報提供システム。

【請求項１４】　前記中継装置は、要求元ユーザのデジタルコンテンツへのアクセスに際して、アクセスに対する課金のためのアクセス記録を採取する手段を備えることを特徴とする請求項１～１３のいずれか一項に記載の情報提供システム。

【請求項１５】　前記中継装置は、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする請求項２記載の情報提供システム。

【請求項１６】　前記要求元装置は、前記中継装置から受信した暗号化されたデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で復号する復号処理手段と、復号されたデジタルコンテンツデータを出力する手段と、出力された前記デジタルコンテンツのハードコピーを禁止する手段を備えることを特徴とする請求項１５記載の情報提供システム。

【請求項１７】　前記要求元装置は、デジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵

を用いて暗号化して２次記憶装置に保管する手段を備えることを特徴とする請求項１６記載の情報提供システム。

【請求項１８】　コンピュータが保持している提供対象のデータをネットワークを介して要求元装置に転送する装置であって、

ネットワークを介して前記コンピュータが保持している提供対象データに対する要求元装置からの転送要求を受付け、当該要求元装置またはユーザのアクセス権限の認証を行なう手段と、アクセス権限の認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する手段を備えることを特徴とする情報提供中継装置。

【請求項１９】　要求元装置に転送する第１の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする請求項１８記載の情報提供中継装置。

【請求項２０】　要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする請求項１８記載の情報提供中継装置。

【請求項２１】　ネットワーク上のコンピュータが保持しているデータに対するアクセス権限の認証を行なう中継装置を介してアクセスし、出力する情報処理装置であって、

アクセス権限の認証を必要とする第１の提供対象データを出力する第１の出力手段と、アクセス権限の認証を必要としない第２の提供対象データを出力する第２の出力手段と、アクセス対象のデータの転送要求を前記中継装置に送信する手段と、前記中継装置におけるアクセス権限の認証結果に応じて当該中継装置を介してアクセス対象のデータを受信する手段と、受信したデータが前記第１の提供対象データであれば前記第１の出力手段を起動して出力させる手段とを備えることを特徴とする情報処理装置。

【請求項２２】　前記第１の提供対象データが要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化されたものであり、該暗号化された第１の提供対象データを復号した後に前記第１の出力手段に出力させる復号処理手段を備えることを特徴とする請求項２１記載の情報処理装置。

【請求項２３】　前記第１の提供対象データがデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で暗号化したものであり、該暗号化された第１の提供対象データを復号した後に前記第１の出力手段に出力させる復号処理手段を備えることを特徴とする請求項２１記載の情報処理装置。

【請求項２４】　前記暗号化された第１の提供対象データを保管する２次記憶装置と、前記第１の出力手段に出力された第１の提供対象データのハードコピーを禁止する手段と、自装置内のアプリケーションから前記２次記憶装置への入出力を監視し、前記第１の出力手段を介在しない第１の提供対象データに対するアクセスを禁止する２次記憶アクセス制御手段とを備えることを特徴とする請求項２３記載の情報処理装置。

【請求項２５】　前記ハードコピーを禁止する手段及び前記２次記憶アクセス制御手段が共に正常に動作していない限り前記第１の出力手段を起動させない手段を備えることを特徴とする請求項２４記載の情報処理装置。

【請求項２６】　自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第１の提供対象データを暗号化して前記２次記憶装置に保管する手段とを備えることを特徴とする請求項２４記載の情報処理装置。

【請求項２７】　要求元ユーザの機密情報を元に生成された固有の鍵を用いて前記第１の提供対象データを暗号化して２次記憶装置に保管する手段を備えることを特徴とする請求項２４記載の情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する分野】本発明は、ネットワーク上に配置されたコンピュータ、例えばWebサーバ上に保管された情報をクライアントコンピュータなどの端末装置からの要求に応じて転送（または配布）し、ユーザの閲覧に供する情報提供システムに係り、特に、機密情報を正当なアクセス権限を有する者以外に漏洩することなく閲覧可能にする情報提供システムおよび装置に関するものである。

【０００２】

【従来の技術】インターネットの需要が高まるにしたがい、インターネット上で送受信される情報を保護する必要性が要求されている。例えば、一般企業等において、顧客情報や人事管理情報などの機密情報を蓄積したデータベースをWebサーバ上に構築し、社内の特別の権限を付与された者のみが自由に閲覧できるようにするシステムをインターネットの利用により容易に実現することができる。しかしながら、インターネットでは回線を盗聴したり、機密情報の蓄積されたデータベースに不正にアクセスすることにより、機密情報が盗まれる恐れがある。また、機密情報にアクセスすることを許された特権のある人物が機密情報にアクセスしてその機密情報をコピーし、第３者に漏洩してしまう事件も発生している。このようなことから、インターネット上のWebサーバ等に蓄積された機密情報を正当なアクセス権限を有する者以外に漏洩することなく閲覧可能にするシステムの実現が強く望まれている。

【０００３】従来、機密情報を管理し漏洩を防止するシステムとして、例えば特開平１１－３２８１２０号公報に記載のものが知られている。特開平１１－３２８１２

０号公報に記載のものは、端末装置の入出力機器の構成や利用者等のデータによって、機密情報の格納されたデータベースへのアクセス権を予め設定し、データベース内の機密情報の漏洩を防ぐためのネットワークシステムである。

【０００４】具体的に図４０を用いて説明すると、ホストコンピュータＡ０２は端末装置Ａ０５からの通信要求を受けると、照合部Ａ０９にて利用者識別子記憶部Ａ０８に登録されている利用者識別子との照合を行なう。照合結果が一致すると、端末装置Ａ０５へハードウェア構成情報を要求する。端末装置Ａ０５からハードウェア構成情報を受信すると、照合部Ａ０９にて端末構成情報記憶部Ａ１０に記憶されているハードウェア構成情報と照合を行い、照合結果が一致すると、端末装置Ａ０５のデータベースＡ１１、Ａ１２へのアクセス権の有無を判定部Ａ１３に行なわせる。判定部Ａ１３から判定結果を受けた制御部Ａ１５は以後、端末装置Ａ０５にアクセス権の有るデータベースの使用を許可するというシステムである。

【０００５】一方、デジタルコンテンツに課金して、利用者に配信するサービスはすでにWeb上で試みられている。例えば、利用者がWebブラウザを使用してバーチャルモール等のデジタルコンテンツ配信ページにアクセスし、バーチャルモールに置かれたデジタルコンテンツを、Webブラウザを使用してダウンロードする方式がある。この方式では、利用者は予めデジタルコンテンツ配信を行っているサイトの管理会社にデジタルコンテンツ配信サービスを受けるための登録を行なう。登録はクレジットカード等の情報を使用してWeb上で行なう方法や、申請書を郵送で送付する方法などがある。登録が済むと、サイトの管理会社からデジタルコンテンツにアクセスするためのＩＤとパスワードが発行される。デジタルコンテンツはWebサーバに保管されており、デジタルコンテンツにアクセスするためにはProxyサーバ経由でアクセスしなければならない。アクセス時に、利用者はＩＤとパスワードによりProxyサーバで認証され、認証が成功すれば利用者はデジタルコンテンツにアクセスできる。

【０００６】しかしながら、この方式における重大な問題点として、利用者によるデジタルコンテンツの不正な二次利用・再配布が考えられる。すなわち、Webブラウザでダウンロードしたデジタルコンテンツをファイルとして保存し、そのファイルをホームページに掲載する、もしくはＦＴＰやメール等を利用して配布する等の行為である。このような行為により、コンテンツ料金を支払っていないにも拘わらず、そのデジタルコンテンツを使用できるユーザが現れ、デジタルコンテンツの課金サービスが成立しない。

【０００７】この問題点に対する解決策として、デジタルコンテンツに電子透かしを入れる方法が考えられる。例えば画像コンテンツの場合、画像データに独自のロゴを埋め込む可視の電子透かしや、輝度の変化を利用して画像データに目立たない形で情報を埋め込む不可視の電子透かしなどがある。また、コンテンツの利用条件に違反した二次利用や不正な再配布を防止する従来技術として、特願平１０－１９０３４３号には、電子透かしの著作物への埋め込みとその検出についての技術が開示されている。

【０００８】

【発明が解決しようとする課題】しかしながら、上記の特開平１１－３２８１２０号公報に記載のものは、一般のWebサーバ１１上に構築されたデータベース対して適用する場合、既存のWebサーバを改変せねばならず、現在運用されている一般的なWebサーバ上のデータベースに適用するには手間がかかるという問題がある。また、Webサーバには、通常、機密情報以外に一般に閲覧するページも存在しており、こうした一般のページの閲覧に対応できない。さらに、ハードウェア構成により機密ファイルのダウンロードを許可する仕組みであるため、適切なハードウェア条件を満たしていなければ、機密ファイルを閲覧することができず、閲覧した機密情報データを一時的に端末に保持しておく機構もない。

【０００９】一方、上述の電子透かしによるデジタルコンテンツの二次利用・再配布を防止する方式にはいくつかの課題がある。まず、透かしを除去して配信する可能性がある。可視の電子透かしの場合にはこの脅威に対する解決策はなく、あくまで抑止効果を期待しているに過ぎないといえる。不可視な電子透かしについては、透かしの除去は困難であるが、一般的に画像データの回転処理や部分的な切り取り等の加工処理に対して弱いとされており、そのような加工処理により電子透かしが検出できなくなったという例も報告されている。また、不正な二次利用・再配布を摘発するために、インターネット上にある画像データに透かしがあるかどうかを検出する必要があるが、検出するための有効な方法が確立されていない。さらに、記録媒体に記録して、オフラインでデジタルコンテンツを配布する場合に対しては、透かしの効果はまったく期待できない。従って、電子透かしを利用した二次配信の防止は抑止効果を期待した消極的な方法であると言える。

【００１０】本発明の第１の目的は、既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置（または端末）のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能にすることができる情報提供システムおよび装置を提供することにある。

【００１１】本発明の第２の目的は、閲覧した機密情報を第３者に漏洩しないように要求元装置内に保存・管理

することができる情報提供システムおよび装置を提供することにある。本発明の第３の目的は、デジタルコンテンツをダウンロードした利用者がダウンロードに使用したマシンでしかデジタルコンテンツを利用できず、ダウンロードしたデジタルコンテンツの不正な二次利用・再配布を防止することができる情報提供システムおよび装置を提供することにある。

【００１２】

【課題を解決するための手段】上記の第１の目的を達成するために、本発明は、ネットワークを介してコンピュータ（例えばWebサーバ）が保持している提供対象データに対する要求元装置（例えばクライアントコンピュータ）からの転送要求を受付け、当該要求元装置自身または要求元ユーザのアクセス権限の認証を行い、その認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する中継装置を備えることを特徴とする。また、前記コンピュータはアクセス権限の認証を必要とする第１の提供対象データと認証を必要としない第２の提供対象データとを保持するものであり、前記中継装置は前記第１の提供対象データに対する転送要求受付け時にアクセス権限の認証を行なうことを特徴とする。また、前記中継装置は、要求元装置に転送する第１の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信した暗号化された第１の提供対象データを自装置または要求元ユーザに固有の暗号鍵に対応した復号鍵で復号する復号処理手段と、復号された第１の提供対象データを表示する第１の表示手段と、中継装置から受信した前記第２の提供対象データを表示する第２の表示手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信したデータに付加されている識別子により第１の提供対象データであるか、第２の提供対象データであるかを判定し、第１の提供対象データである場合に前記第１の表示手段を起動する手段と、第１の表示手段が正常に起動できなければ中継装置から受信した第１の提供対象データを削除する手段とを備えることを特徴とする。

【００１３】上記第２の目的を達成するために、前記要求元装置は、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第１の提供対象データを暗号化して２次記憶装置に保管する手段とを備えることを特徴とする。また、前記要求元装置は、前記第１の出力手段に出力された第１の提供対象データのハードコピーを禁止する手段を備えることを特徴とする。また、前記要求元装置は、要求元装置内のアプリケーションから前記２次記憶装置への入出力を監視し、前記第１の出力手段を介在しない第１の提供対象データに対するアクセスを禁止する２次記憶アクセス制御手段とを備えることを特徴とする。また、前記要求元装置は、前記ハードコピーを禁止する手段及び前記２次記憶アクセス制御手段が共に正常に動作していない限り前記第１の出力手段を起動させない手段を備えることを特徴とする。また、前記中継装置および要求元装置は、要求元装置のユーザのアクセス権限の認証を行なうためのアクセス権限判定用情報を記憶した第１の記憶手段をそれぞれ備えることを特徴とする。また、前記要求元装置は、前記２次記憶装置に保管された第１の提供対象データへのアクセスの都度または所定の時期に、前記中継装置内の前記第１の記憶手段に記憶されたアクセス権限判定用情報を取得し、自装置内の第１の記憶手段に記憶されているアクセス権限判定用情報を最新バージョンに更新する手段とを備え、更新されたアクセス権限判定用情報により、前記２次記憶装置に保管された第１の提供対象データへのアクセス権限の有無を判定することを特徴とする。また、前記中継装置は、要求元装置からユーザ識別情報を取得してアクセス権限の認証を行なうことを特徴とする。また、前記中継装置は、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信した暗号化されたデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で復号する復号処理手段と、復号されたデジタルコンテンツデータを出力する手段と、出力された前記デジタルコンテンツのハードコピーを禁止する手段を備えることを特徴とする。また、前記要求元装置は、デジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化して２次記憶装置に保管する手段を備えることを特徴とする。

【００１４】上記第３の目的を達成するために、本発明における要求元装置は、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第１の提供対象データを暗号化して２次記憶装置に保管する手段とを備えることを特徴とする。また、前記中継装置は、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする。また、前記要求元装置は、前記中継装置から受信した暗号化されたデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で復号する復号処理手段と、復号されたデジタルコンテンツデータを出力する手段と、出力された前記デジタルコンテンツのハードコピーを禁止する手段を備えることを特徴とする。また、前記要求元装置は、デジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化して２次記憶装置に保管する手段を備えることを特徴とする。

【００１５】本発明の情報提供中継装置は、ネットワークを介して前記コンピュータが保持している提供対象データに対する要求元装置からの転送要求を受付け、当該要求元装置またはユーザのアクセス権限の認証を行なう手段と、アクセス権限の認証結果に応じて前記提供対象データを前記コンピュータから取得し、要求元装置にネットワークを介して転送する手段を備えることを特徴とする。また、要求元装置に転送する第１の提供対象データを要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化する手段を備えることを特徴とする。また、要求元装置に転送するデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵を用いて暗号化する手段を備えることを特徴とする。

【００１６】また、要求元装置を構成する情報処理装置は、アクセス権限の認証を必要とする第１の提供対象データを出力する第１の出力手段と、アクセス権限の認証を必要としない第２の提供対象データを出力する第２の出力手段と、アクセス対象のデータの転送要求を前記中継装置に送信する手段と、前記中継装置におけるアクセス権限の認証結果に応じて当該中継装置を介してアクセス対象のデータを受信する手段と、受信したデータが前記第１の提供対象データであれば前記第１の出力手段を起動して出力させる手段とを備えることを特徴とする。また、前記第１の提供対象データが要求元装置または要求元ユーザに固有の暗号鍵を用いて暗号化されたものであり、該暗号化された第１の提供対象データを復号した後に前記第１の出力手段に出力させる復号処理手段を備えることを特徴とする。また、前記第１の提供対象データがデジタルコンテンツを要求元ユーザの機密情報を元に生成された固有の鍵で暗号化したものであり、該暗号化された第１の提供対象データを復号した後に前記第１の出力手段に出力させる復号処理手段を備えることを特徴とする。また、前記暗号化された第１の提供対象データを保管する２次記憶装置と、前記第１の出力手段に出力された第１の提供対象データのハードコピーを禁止する手段と、自装置内のアプリケーションから前記２次記憶装置への入出力を監視し、前記第１の出力手段を介在しない第１の提供対象データに対するアクセスを禁止する２次記憶アクセス制御手段とを備えることを特徴とする。また、前記ハードコピーを禁止する手段及び前記２次記憶アクセス制御手段が共に正常に動作していない限り前記第１の出力手段を起動させない手段を備えることを特徴とする。また、自装置固有の情報を元に自装置固有の鍵情報を生成する手段と、該手段によって生成された鍵情報および要求元ユーザ固有の暗号鍵のいずれか一方または両方を用いて前記第１の提供対象データを暗号化して前記２次記憶装置に保管する手段とを備えることを特徴とする。また、要求元ユーザの機密情報を元に生成された固有の鍵を用いて前記第１の提供対象データを暗号化して２次記憶装置に保管する手段を備えることを特徴とする。

【００１７】

【発明の実施の形態】以下、本発明を実施する場合の一形態を図面を参照して具体的に説明する。図１は、本発明の情報提供システムの第１の実施形態を示す全体構成図であり、大別すると、Webサーバ１１、ルータ１２、ネットワーク１３、クライアントコンピュータ（以下、Clientと略記）１４およびProxyサーバ２０で構成されている。Client１４は、Browser１５、ハードコピー禁止モジュール１６、２次記憶装置１７、２次記憶装置アクセス制御部１８、アクセストークン１９、通信フックモジュール３０、外部Viewer４０を備えている。

【００１８】Webサーバ１１は、アクセス権限の認証を必要とする機密ファイル（第１の提供対象データ）５０とアクセス権限の認証を必要としない非機密ファイル（第２の提供対象データ）５１を保管している。このWebサーバ１１とProxyサーバ２０は、同じセグメント上に配され、ルータ１２によってネットワーク１３から隔離されている。従って、機密ファイル５０へのアクセスを行なうためには、必ずProxyサーバ２０を経由しなければならない。Client１４が機密ファイル５０にアクセスしたとき、機密ファイル５０は一旦Proxyサーバ２０にダウンロードされ、Client１４ごとに用意された共通鍵を用いて動的に暗号化される。

【００１９】Webサーバ１１上には機密ファイル５０を予め暗号化して保管しておく必要はない。暗号化された機密ファイル５０はClient１４に送信され、通信フックモジュールにおいて復号された後、専用の外部Viewer（第１の表示手段）４０に表示される。Client１４内では、ユーザごとに設けられたフォルダに、対応するユーザでシステムにログインし、専用の外部Viewer４０でしかアクセスできないようなアクセス制御をＯＳレベルで行なうようになっている。従って、ユーザごとに機密ファイルの管理が行なえる機構を備えたシステムであると言える。

【００２０】次に、各構成要素について説明する。Webサーバ１１はＨＴＴＰプロトコルもしくはＦＴＰプロトコル等によってClient１４よりProxyサーバ２０経由で送られるファイルのダウンロード要求を処理し、Client１４にファイルを転送する機能を有するものであり、同時にユーザ認証も行なう。ルータ１２は、ＩＰパケットの宛先ＩＰアドレスによるフィルタリングを行っており、Proxyサーバ２０へ送信されるＩＰパケットのみ通過させるように設定されている。従って、Webサーバ１１へのアクセスは、すべてProxyサーバ２０を介して行われる。Proxyサーバ２０はClient１４からのアクセスを解析し、機密ファイル５０へのアクセスの場合にはダウンロードした機密ファイル５０をClient１４ごとに用意された共通鍵を用いて暗号化し、Client１４に転送する。Browser１５は、Webサーバ１１からダウンロードし

たファイル、又はプログラムを表示、ないしは実行するためのアプリケーションであり、機密ファイル５０以外の一般のファイル５１を閲覧する際に使用する。

【００２１】通信フックモジュール３０は、Proxyサーバ２０にClient１４を認証させるためのClientマシン識別子を付加してファイルのＧＥＴリクエストを送信し、ダウンロードされた暗号化された機密ファイル５０を復号する。外部Viewer４０は、機密ファイル５０がダウンロードされてきた際に通信フックモジュール３０によって起動され、復号された機密ファイル５０を表示し、２次記憶装置１７に保存したり、読み出す処理を行なう。ここで、外部Viewer４０は表示データのコピー機能（マウスカーソルによる選択、もしくはDrag&Dropによるコピー）を実装しない。ハードコピー禁止モジュール１６は、外部Viewer４０が起動されると同時に起動され、終了すると同時に終了するモジュールであり、システムコールをフックする機能を利用することにより（例えばWindows NTではWin32 Hooksを利用）、ハードコピーを禁止する機能を有する。

【００２２】２次記憶装置アクセス制御部１８は、ＯＳの起動時にロードされるモジュールであり、アプリケーションが２次記憶装置１７にアクセスする際に出される入出力要求を途中で捕獲し解析し、アクセス要求ファイル、アクセス要求アプリケーションを確定し、特定のフォルダ内のファイルに対するアクセスの場合には外部Viewer４０のみにしかアクセスできないように制限を加える。フォルダは機密ファイル閲覧者ごとに用意されており、２次記憶装置アクセス制御部１８はアクセストークン１９を調べることにより、ユーザアカウントごとにも各フォルダに対してアクセス制限をかける機能を有する。アクセストークン１９は、ユーザがClient１４にログインした時点でＯＳ内部に生成されるオブジェクトであり、ＯＳにおけるユーザのログイン情報を管理し、ＯＳの機能として持つファイルへのユーザごとのアクセス制限のためにも使用される。

【００２３】図２は、本発明におけるProxyサーバ２０のブロック構成図である。Proxyサーバ２０は、Client１４とProxyサーバ２０間の通信を司るClient－Proxy間通信制御部２１と、Webサーバ１１上に保管されている機密ファイル５０のＵＲＬが登録されている機密ファイルＵＲＬ登録部２２と、通信フックモジュール３０を有するClient１４を認証するためのClientマシン識別子が格納されたClientマシン識別子データベース２３と、Client１４から送信されたデータを解析して、機密ファイル５０へのアクセスかどうかを判定するProxy内受信データ解析部２４と、Client１４から送られたデータ内にClientマシン識別子があるかどうかを判定するClientマシン認証部２５と、Webサーバ１１とProxyサーバ２０間の通信を司るWeb－Proxy間通信制御部２６と、Proxyサーバ２０からClient１４への送信ファイルが機密ファイル５０を暗号化したものであることをClient１４に知らせるために識別子を付加する機密ファイル識別子付加部２７と、Webサーバ１１からダウンロードした機密ファイル５０を暗号化する機密ファイル暗号化部２８と、暗号化のためにClient１４ごとに用意された共通鍵を管理する共通鍵データベース２９で構成されている。

【００２４】図３は、Client１４内に設けた通信フックモジュール３０のブロック構成図である。図３において、Proxy－通信フックモジュール間通信制御部３１は、Proxyサーバ２０と通信フックモジュール３０との間の通信を司る部分である。機密ファイル識別子格納部３２は、Proxyサーバ２０において、機密ファイル５０に付加された機密ファイル識別子を照合するために、予め識別子のコピーを格納しておく部分である。また、受信データ解析部３５は、通信フックモジュール３０が受信したデータを解析し、データ内に暗号化された機密ファイル５０であることを示す機密ファイル識別子が存在するか否かを確認するものであり、機密ファイル識別子が存在すれば、受信データ解析部３５は受信データを暗号化ファイル復号部３３に渡し、機密ファイル識別子が存在しなければ、受信データを内部アプリケーション－通信フックモジュール間通信制御部３７に渡す。

【００２５】暗号化ファイル復号部３３は、共通鍵格納部３４に格納されているClient１４固有の共通鍵を用いて、暗号化された機密ファイル５０を復号する。送信データ解析部３６は、ＧＥＴリクエストの送信先ＵＲＬを調べて、Proxyサーバ２０への送信の場合はClientマシン識別子付加部３８に送信データを渡す。Clientマシン識別子付加部３８は、送信データに各Client１４固有のClientマシン識別子を付加する。外部Viewer起動処理部３９は、暗号化ファイル復号部３３より要請を受けて、外部Viewer４０を起動し、起動できたかどうかを暗号化ファイル復号部３３に知らせる。

【００２６】図４はClient１４内に設けた外部Viewer４０のブロック構成図である。図４において、通信フックモジュール－Viewer間通信制御部４１は、通信フックモジュール３０と外部Viewer４０との間の通信を司るものである。機密ファイル表示部４２は、機密ファイルキャッシュ部４３にキャッシュされた機密ファイル５０を表示するものである。機密ファイルキャッシュ部４３は外部Viewer４０に転送された機密ファイル５０を一時的に保存しておく所である。機密ファイルアクセス・保存処理部４４は、機密ファイルキャッシュ部４３にキャッシュされている機密ファイル５０を２次記憶装置１７内に保存したり、２次記憶装置１７内に保存されている機密ファイル５０にアクセスしたりする。

【００２７】外部Viewer起動判定部４７は、ハードコピー禁止モジュール起動処理部４５、及び２次記憶装置アクセス制御部起動処理部４６にアクセスして、ハードコピー禁止モジュール１６を起動、また２次記憶装置アク

セス制御部１８が起動しているか否かの確認を行い、通信フックモジュール３０に通知する。

【００２８】次に、本実施形態における各モジュール間の処理の流れや関連を説明する。図５はProxyサーバ２０における処理のフローチャートを示したものである。Proxyサーバ２０は、Client１４からのアクセスがあると（ステップ５０１）、Proxy内受信データ解析部２４で受信したデータの解析を行い、アクセス要求ファイルのＵＲＬやClientマシン識別子の有無等を調べる（ステップ５０２）。そしてアクセス要求ファイルのＵＲＬと機密ファイルＵＲＬ登録部２２にある機密ファイルＵＲＬのデータをもとに、機密ファイル５０へのアクセス要求であるかどうか調べる（ステップ５０３）。機密ファイル５０へのアクセスでない場合、受信データにClientマシン識別子があればそれを除去し、なければそのままの状態で、Webサーバ１１に転送する。

【００２９】Webサーバ１１では、ユーザ認証が行われ、認証が通ればWebサーバ１１から非機密ファイル５１がダウンロードされる（ステップ５１１）。その後、ダウンロードした非機密ファイル５１をそのままClient１４に転送する（ステップ５１２）。

【００３０】アクセス権限の認証を必要とする機密ファイル５０へのアクセスである場合、Clientマシン識別子が検出されていれば、Proxy内受信データ解析部２４はそのClientマシン識別子をClientマシン認証部２５に渡し、Clientマシン認証部２５においてClientマシン識別子データベース２３をもとにClientマシン認証を行なう（ステップ５０４）。Clientマシン識別子がClient１４からの受信データに付加されていなければ、本発明のシステムにおける正当なClient１４からのアクセスでないと判断して、機密ファイル５０へのアクセスを拒否する。また、Clientマシン認証部２５においてClientマシンが認証されない場合も同様に機密ファイル５０へのアクセスを拒否する（ステップ５０６）。

【００３１】Clientマシン識別子が照合され、アクセス要求を行ったClient１４がClientマシン識別子データベース２３に予め登録されている正当なClientマシンであると認証された場合、Clientマシン認証部２５から通知を受けたProxy内受信データ解析部２４は、Clientマシン識別子を除去した受信データをWebサーバ１１に転送し、Webサーバ１１から該当する機密ファイル５０をダウンロードする（ステップ５０７）。

【００３２】この後、機密ファイル暗号化部２８にて、ダウンロードした機密ファイル５０を共通鍵データベース２９にあるClient１４に対応した共通鍵を用いて暗号化し（ステップ５０８）、さらに機密ファイル識別子付加部２７にて暗号化された機密ファイルに機密ファイル識別子を付加した後（ステップ５０９）、その暗号化され、かつ識別子の付加された機密ファイルをClient１４に転送する（ステップ５１０）。なお、共通鍵データベース２９内のClient１４に対応した共通鍵を検索するときは、Clientマシン認証部２５から得たClient１４の認証結果をもとに行なう。共通鍵データベース２９内の共通鍵とClientマシン識別子とは１対１に対応付けられている。

【００３３】図６は、Client１４内の通信フックモジュール３０におけるデータ送信時の一連の処理を記述したフローチャートである。まず、Browser１５からネットワーク１３へデータが送信された場合、内部アプリケーション－通信フックモジュール間通信制御部３７にてそのデータを受信し（ステップ６０１）、送信データ解析部３６で送信データを解析し、送信先がProxyサーバ２０であるかどうかを調べる（ステップ６０２）。Proxyサーバ２０への送信でなければ、送信データをネットワーク１３にそのまま転送する（ステップ６０４）。Proxyサーバ２０への送信であれば、Clientマシン識別子付加部３８において送信データにClientマシン識別子を付加した後（ステップ６０５）、Proxyサーバ２０に送信データを転送する（ステップ６０６）。

【００３４】図７は、通信フックモジュール３０において、データ受信時における処理のフローチャートである。通信フックモジュール３０は、Proxy－通信フックモジュール間通信制御部３１でネットワーク１３からClient１４に送られてきたデータを受信したならば（ステップ７０１）、受信データ解析部３５で受信データに機密ファイル識別子があるかないかを解析する（ステップ７０２、７０３）。受信データから機密ファイル識別子が検出されなかった場合、そのままBrowser１５に受信データを転送する（ステップ７０９）。しかし、機密ファイル識別子が検出された場合、暗号化ファイル復号部３３にて、機密ファイル識別子を除去し、共通鍵格納部３４に格納されているClient１４に固有の共通鍵を用いて暗号化された機密ファイル５０を復号する（ステップ７０４）。そして外部Viewer４０起動処理部３９により外部Viewer４０が起動していなければ起動させ、外部Viewer４０が正常に起動したかどうか確認させる（ステップ７０５、７０６）。外部Viewer４０の起動を試みたのに起動していなければ受信データを削除する（ステップ７０７）。外部Viewer４０が正常に起動していれば、復号された機密ファイル５０のデータを外部Viewer４０に転送して表示させる（ステップ７０８）。

【００３５】図８は、２次記憶装置アクセス制御部１８における機密ファイルアクセス時の処理のフローチャートである。２次記憶装置１７にはユーザごとに用意された機密ファイル保存用の特別なフォルダがあるとする。このフォルダは各ユーザのアカウントと一緒に２次記憶装置アクセス制御部１８に登録されているものであり、この登録データをもとに２次記憶装置アクセス制御部１８は、Client１４にログインしているユーザがこのフォルダにアクセスできるかどうかを判定する。Client１４

内のアプリケーションから、２次記憶装置１７の特定のフォルダに保存された機密ファイル５０へのアクセス要求があったとき、機密ファイル５０へのＩ／Ｏアクセス要求がシステム内部で出され、２次記憶装置１７に送られるが、２次記憶装置アクセス制御部１８はそのＩ／Ｏアクセス要求を途中でフックし、その内容を解析する（ステップ８０１）。この解析により、Ｉ／Ｏアクセス要求を行っているアプリケーションとアクセス要求フォルダを調べる。２次記憶装置アクセス制御部１８はアクセストークン１９にアクセスし、ログインユーザ情報を取得する（ステップ８０２）。

【００３６】アクセス要求アプリケーションが外部Viewer４０であるかどうか、アクセス要求対象のフォルダがログインユーザに対応しているかどうかを判定し、アクセス要求対象のフォルダ内の機密ファイルへアクセスしてよいかどうかを判定する。アクセス要求対象のフォルダがログインユーザに対応しているかどうかは、予め２次記憶装置アクセス制御部１８にある、機密ファイル保存用フォルダへのパスとそのフォルダにアクセス可能なユーザのユーザアカウントの対データが登録されているデータベース（図示せず）を検索することで判定する（ステップ８０３）。アクセス可能であるならば、機密ファイル５０へのアクセスを許可してＩ／Ｏアクセス要求を２次記憶装置１７のデバイスドライバに渡す（ステップ８０５）。アクセス不可能の判定が出たならば、機密ファイル５０へのアクセスを禁止する（ステップ８０６）。

【００３７】なお、２次記憶装置１７に格納された機密ファイル５０へのアクセスの判定条件は、アクセス要求しているアプリケーションが外部Viewer４０であり、かつアクセス要求対象の機密ファイル格納フォルダがログインユーザに対応している場合にのみアクセスを許すものとする。すなわち、機密ファイル格納フォルダがログインユーザに対応している場合であっても、外部Viewer４０が起動していない状態では、２次記憶装置１７に格納された機密ファイル５０へのアクセスは許可しない。また、外部Viewer４０が起動している状態であったとしても、機密ファイル格納フォルダがログインユーザに対応していない場合もアクセスを許可しない。

【００３８】図９は、外部Viewer４０における受信データ表示処理のフローチャートである。外部Viewer４０は、通信フックモジュール３０から起動要求を受ける、またはユーザから起動要求を受けると（ステップ９０１）、２次記憶装置アクセス制御部起動処理部４６で、２次記憶装置アクセス制御部１８が動作しているかどうか調べる（ステップ９０２）。動作していなければ、外部Viewer４０起動判定部４７は、通信フックモジュール３０にエラーを通知し（ステップ９０３）、外部Viewer４０の起動を終了する（ステップ９０４）。動作していれば、外部Viewer４０は、ハードコピー禁止モジュール起動処理部４５でハードコピー禁止モジュール１６の起動を試みる（ステップ９０５）。起動しなければ、外部Viewer起動判定部４７は通信フックモジュール３０にエラーを通知し（ステップ９０９）、外部Viewer４０の起動を中止する（ステップ９１０）。ハードコピー禁止モジュール１６が起動すれば、通信フックモジュール３０から復号された機密ファイル５０を受信し（ステップ９０７）、その受信データを表示する（ステップ９０８）。

【００３９】このように外部Viewer４０起動の際に、ハードコピー禁止モジュール１６が起動するかどうか判定し、さらに２次記憶装置アクセス制御部１８が正常に動作していることを確認することによって、外部Viewer４０が復号された機密ファイル５０のデータを表示する際に、機密データのハードコピーが撮られてしまうことを不可能にすることができる。さらに、予め２次記憶装置アクセス制御部１８に登録してある機密ファイル格納フォルダ内に保存されている機密ファイルが別のフォルダにコピーできないことを保障することができる。そして、その機密ファイル格納フォルダには外部Viewer４０でしかアクセスできないので、他のアプリケーションによって機密ファイル格納フォルダに保存された機密ファイルにアクセスすることができない。また、外部Viewer４０が起動しなければ通信フックモジュール３０は復号した機密ファイルを削除してしまうので、Client１４内の他のアプリケーションには機密ファイル５０にアクセスする手段がなく、機密データが外部に漏洩することはない。

【００４０】なお、ユーザが外部Viewer４０を起動した場合には、ステップ９０３と９０９の通信フックモジュールへのエラー通知は行なわない。

【００４１】以上説明したように、本実施形態の情報提供システムは、機密ファイル５０と非機密ファイル５１を保管したWebサーバ１１に対し、Client１４からの機密ファイル５０へのアクセス要求があった場合、Client１４から送信されたアクセス要求（転送要求）に付加されているClientマシン識別子をもとにClient１４の認証を行い、アクセス権限を有するClient１４であれば、要求された機密ファイル５０をWebサーバ１１からダウンロードし、その機密ファイルをアクセス要求元のClient１４に固有の共通鍵を用いて暗号化し、さらに暗号化ファイルであることを示す機密ファイル識別子を付加し、アクセス要求元のClient１４に転送するProxyサーバ２０を備えることを特徴とする。

【００４２】このような構成により、既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置（または端末）のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能に

することができる。

【００４３】また、Client１４において、Webサーバ１１上の一般の非機密ファイル５１を閲覧するためのBrowser１５と、機密ファイル５０を閲覧し、２次記憶装置１７に保存する手段を備えた外部Viewer４０と、Client１４内の任意のアプリケーションとネットワーク１３との通信を中継し、暗号化された機密ファイル５０を受信した際に外部Viewer４０を起動し、起動できなければ機密ファイル５０を削除する手段と、Client１４からProxyサーバ２０へのデータ送信の際にClientマシン識別子を送信データに付加する手段と、Proxyサーバ２０から送信された暗号化された機密ファイルを識別してClient１４に固有の復号鍵で暗号化された機密ファイルを復号し、外部Viewer４０に転送する手段と、機密ファイル５０以外のファイルが転送されてきたとき、それを判定してBrowser１５にそのデータを転送する手段とを備えた通信フックモジュール３０と、ログインユーザ情報を格納したアクセストークン１９と、機密情報を格納するための２次記憶装置１７と、アクセストークン１９からログインユーザ情報を取得する手段と、Client１４内のアプリケーションから２次記憶装置１７へのＩ／Ｏを監視して、ファイルへのアクセス要求を行っているアプリケーションとそのアクセス要求ファイルを特定する手段と、特定のフォルダに対して、特定のログインユーザが外部Viewer４０でアクセスする以外にはアクセスを禁止する手段とを備えた２次記憶装置アクセス制御部１８と、外部Viewer４０起動中に外部Viewer４０に表示されている画面のハードコピーを禁止する手段を備えたハードコピー禁止モジュール１６とを有することを特徴とする。さらに、外部Viewer４０は、ハードコピー禁止モジュール１６及び２次記憶装置アクセス制御部１８が共に正常に動作していない限り起動しない手段を備えることを特徴とする。

【００４４】このような構成により、閲覧した機密ファイル５０を第３者に漏洩しないようにアクセス要求元のClient１４内に保存・管理することができる。また、機密ファイル５０はClient１４ごとに決められた共通鍵を用いて暗号化されて要求元のClient１４に送信されるので、Client１４とProxyサーバ２０間の通信回線上で盗聴される恐れがなくなる。また、ダウンロードした機密ファイル５０は、ユーザごとに所定のフォルダに安全に保管され、なおかつ保管された機密ファイル５０は外部Viewer４０以外のアプリケーションではアクセスできないために、コピーされて外部に持ち出されることもない。さらに外部Viewer４０起動中にはハードコピー禁止モジュール１６が起動しているため、外部Viewer４０に表示されている機密データのハードコピーをとることもできなくなり、アクセス権限を有するユーザであったとしても機密データをコピーして外部に持ち出すことは不可能になる。

【００４５】なお、Proxyサーバ１１に対するアクセス要求にはClientマシン識別子を付加しているが、Webサーバ１１における認証の仕方によってユーザ識別子と組み合せる、あるいはユーザ識別子のみにすることができる。また、機密ファイルを暗号化または復号する際の暗号鍵および復号鍵もClient１４に固有のものでなく、アクセスする個々のユーザまたはユーザグループに対応するものであってもよい。また、機密ファイルを暗号化または復号する際の暗号鍵および復号鍵は、Client１４の装置自身に固有の情報（ＭＡＣアドレス、ＩＰアドレス、ＣＰＵ製造番号など）を元に生成した鍵情報、またはユーザ自身の機密情報（例えばクレジット番号など）から生成した鍵情報を用いてもよい。

【００４６】次に、本発明の第２の実施形態について説明する。図１０は、第２の実施形態を示す全体構成図である。この第２の実施形態の情報提供システムは、機密ファイル５０と非機密ファイル５１を保管しているWebサーバ１１と、機密ファイル５０へのアクセス権限を策定すると共に、ユーザ及びマシン認証及びClient１４からの機密ファイル５０へのアクセス要求に従いWebサーバ１１から機密ファイル５０をダウンロードして暗号化し、アクセス要求元のClient１４へ暗号化された機密ファイル５０の転送を行なうProxyサーバ２０と、ルータ１２と、ネットワーク１３と、複数のClient１４によって構成されている。各Client１４は、Proxyサーバ２０から送られた暗号化機密ファイルのファイル名を除去し、キャッシュ、復号化して表示するViewer６０、非機密ファイル５１を表示するBrowser６１、暗号化された機密ファイル５０を復号するためのユーザ固有の復号鍵を格納した復号用共通鍵データベース６２、ユーザ固有の復号用共通鍵と復号用共通鍵を適用するためのポリシを管理する機能をもつポリシ管理モジュール６４及びポリシデータベース６３を備えている。

【００４７】この実施形態においても、前述した第１の実施形態と同様に、Webサーバ１１とProxyサーバ２０は同じセグメント上に配置されており、外部のネットワーク１３とはルータ１２のみを介して接続されている。ルータ１２においては、ＩＰパケットの宛先ＩＰアドレスによるフィルタリングを行っており、Proxyサーバ２０へ送信されるＩＰパケットのみ通過させる。また、各Client１４には、ファイルの拡張子から判断してViewer６０を起動するBrowser６１がインストールされている。

【００４８】図１１は、本実施形態におけるClient１４のブロック構成図である。Client１４は、Viewer６０、Browser６１、復号用共通鍵データベース６２、２次記憶装置６７、ハードウェア固有情報６５、ネットワーク側通信制御部６６、ポリシデータベース６３、ポリシ管理モジュール６４を有している。このうち、Viewer６０はViewer起動判定部６０１１、Viewer内認証用ハードウェア固有情報６０１２、暗号化機密ファイルキャッシュ

部６０１３、機密ファイル名データ除去部６０１４、暗号化機密ファイル復号部６０１５、機密ファイル表示部６０１６、及びViewer内復号用共通鍵キャッシュ部６０１７を備えている。

【００４９】Viewer起動判定部６０１１は予め登録しておいたViewer内認証用ハードウェア固有情報６０１２と、Client１４のハードウェアに固有のデータであるハードウェア固有情報６５（これは例えばＭＡＣアドレスや別途外付けされたハードウェア、ＩＣカード内に貯えられた改竄不可能な特殊データなど）を比較照合し、２つのデータが一致すればViewer６０を起動し、一致しなければViewer６０を起動させない判定を下すモジュールである。暗号化機密ファイルキャッシュ部６０１３は、暗号化機密ファイル５０がBrowser６１から転送された際に、暗号化機密ファイル５０を一時的にキャッシュしておくものである。Viewer６０でファイルを２次記憶装置６７に保存する場合、この暗号化機密ファイルキャッシュ部６０１３にキャッシュされているデータを保存する。このことにより、２次記憶装置６７には機密ファイル５０が暗号化されたまま保存される。保存された機密ファイル５０を参照するときには、この機密ファイル５０を暗号化するために用いられた、ユーザに固有の復号用共通鍵と復号するためのViewer６０、復号可能な設定にあるポリシデータが必要である。従って、２次記憶装置６７に保存された暗号化機密ファイル５０が、Client１４から外部に漏れたとしても、復号用共通鍵データベース６２に保管されるべきユーザ固有の復号用共通鍵、Viewer６０、及びポリシ管理モジュール６４がなければ暗号化機密ファイル５０を閲覧することができず、機密情報が外部に漏れることはない。

【００５０】機密ファイル名データ除去部６０１４は、Proxyサーバ２０で機密ファイル５０であることを表すためにファイル名の付け替えられた暗号化機密ファイル５０がBrowser６１から転送された際、この暗号化機密ファイル５０のファイル名データを除去するモジュールである。暗号化機密ファイル復号部６０１５は、Viewer内復号用共通鍵キャッシュ部６０１７にキャッシュされたユーザ固有の復号用共通鍵を用いて、ファイル名データの除去された暗号化機密ファイル５０を復号するものである。Viewer内復号用共通鍵キャッシュ部６０１７は、ポリシ管理モジュール６４から渡されたユーザ固有の復号用共通鍵を一時的にキャッシュするものである。Browser６１は、Proxyサーバ２０から送られてきた機密ファイル５０をそのファイル名から判断し、Viewer６０を起動して暗号化された機密ファイル５０をViewer６０に転送する。ハードウェア固有情報６５は、ＭＡＣアドレスや別途外付けされたハードウェア、ＩＣカード内の機密データなど、Client１４マシンのハードウェア構成に固有の情報である。ネットワーク側通信制御部６６は、Client１４をネットワーク１３に接続するための通信制御モジュールである。ポリシデータベース６３は、Proxyサーバ２０で管理されている機密ファイル５０へのアクセスポリシ（アクセス権限を判定するための情報）をダウンロードし、暗号化して保管しておくところであり、２次記憶装置６７に保存されている暗号化された機密ファイル５０を閲覧するために、Viewer６０及びポリシ管理モジュール６４を起動する際にProxyサーバ２０と通信して更新される。

【００５１】図１２は、本実施形態におけるProxyサーバ２０のブロック構成図である。Proxyサーバ２０は、Client－Proxy間通信制御部２０１、機密ファイルリスト及びアクセスポリシ登録部２０２、要求ファイルアクセス判定部２０３、受信データ解析部２０４、ユーザ認証部２０５、暗号用共通鍵選択部２０６、機密ファイル暗号部２０７、Web－Proxy間通信制御部２０８、機密ファイルキャッシュ部２０９、機密ファイルＵＲＬ送信部２１０、暗号用共通鍵データベース２１１、及び機密ファイル名変更部２１２を備えている。

【００５２】Client－Proxy間通信制御部２０１は、Client１４との通信を制御するモジュールである。機密ファイルリスト及びアクセスポリシ登録部２０２は、機密ファイル５０へのアクセスが許可されているユーザのユーザＩＤとパスワードの組を管理するテーブル、及び、Webサーバ１１上にある機密ファイル５０の一覧と各ファイル５０へのユーザのアクセス権限を管理するテーブル及びそのテーブルのバージョン情報を保管している。また、Client１４からのポリシバージョン問い合わせに対して、ポリシのバージョンを比較し、Proxyサーバ２０のポリシバージョンのほうが新しいものであれば、ポリシデータをClient１４に送信する機能を備えている。受信データ解析部２０４は、Client１４から受信したデータを解析し、アクセス要求ファイルのＵＲＬを調べるモジュールである。要求ファイルアクセス判定部２０３は、受信データ解析部３０４で獲得したアクセス要求ファイルのＵＲＬと機密ファイルリスト及びアクセスポリシ登録部２０２に登録された機密ファイルのＵＲＬリストから、アクセス要求ファイルが機密ファイル５０かどうか判断するものであり、機密ファイル５０へのアクセスならば、ユーザ認証部２０５はClient１４のポリシ管理モジュール６４内のユーザ・Clientマシン認証部６４２（図１３）に、ユーザ情報を入力するためのダイアログボックスをClient１４のディスプレイに表示する要求を送信し、ユーザにより入力されたユーザＩＤとパスワードを受信し、そのユーザ情報をもとにユーザ認証を行なう。ユーザ認証の結果をもとに、要求ファイルアクセス判定部２０３は機密ファイル５０へのアクセスを許可するかどうか決定する。機密ファイル５０へのアクセスが許可されたならば、要求ファイルアクセス判定部２０３は、Webサーバ１１に対し機密ファイル５０をダウンロードする要求を出す。

【００５３】Client１４の２次記憶装置６７に保存されている暗号化機密ファイル５０にアクセスする際に、Client１４にあるポリシ管理モジュール６４はProxyサーバ２０にポリシバージョンの問い合わせを行なうが、Proxyサーバ２０のユーザ認証部２０５は、ポリシ管理モジュール６４からのポリシバージョンの問い合わせによる通信の際に、ポリシ管理モジュール６４から送信されたユーザＩＤとパスワードをもとにユーザ認証を行う。

【００５４】暗号用共通鍵データベース２１１は、Webサーバ１１上の機密ファイル５０にアクセスできるユーザごとに用意された、ユーザ固有の暗号用共通鍵を保管している。暗号用共通鍵選択部２０６は、ユーザ認証後にユーザに対応する暗号用共通鍵を、暗号用共通鍵データベース２１１から検索して取り出し、機密ファイル暗号部２０７に渡す。機密ファイル暗号部２０７は、Webサーバ１１からダウンロードしてきた機密ファイル５０をファイル名ごと、アクセスしてきたユーザに固有の暗号用共通鍵を用いて暗号化するモジュールである。機密ファイル名変更部２１２は、機密ファイル暗号部２０７で暗号化されたファイルにファイル名を付け、機密ファイルキャッシュ部２０９に送る。機密ファイルキャッシュ部２０９は、暗号化された機密ファイル５０を一時的にキャッシュしておくところであり、認証されたユーザからアクセスがあればそのファイルをアクセス要求元のClient１４に送信する。Web－Proxy間通信制御部２０８は、Proxyサーバ２０とWebサーバ１１間の通信を制御するモジュールである。

【００５５】図１３は、本実施形態におけるClient１４内のポリシ管理モジュール６４のブロック構成図である。ポリシ管理モジュール６４は、通信制御部６４１、ユーザ・Clientマシン認証部６４２、ポリシ管理モジュール内復号用共通鍵キャッシュ部６４３、復号用共通鍵ポリシ判定部６４４、Viewerーポリシ管理モジュール間通信制御部６４５、ポリシ暗号・復号化部６４６、ポリシキャッシュ部６４７、認証用ハードウェア固有情報６４８から構成される。

【００５６】通信制御部６４１は、ポリシ管理モジュール６４とネットワーク側通信制御部６６との間の通信を制御するモジュールである。ユーザ・Clientマシン認証部６４２は、ポリシ適用の際に必要なユーザ及びClientマシンの認証を行い、ユーザ情報をキャッシュする。Clientマシン認証の際には、マシンのハードウェア固有情報６５を参照し、認証用ハードウェア固有情報６４８と照合する。ポリシ管理モジュール内復号用共通鍵キャッシュ部６４３は、復号用共通鍵データベース６２からユーザＩＤをもとに検索したユーザ固有の復号用共通鍵を一時的にキャッシュする。ポリシ暗号・復号化部６４６では、ポリシデータベース６３から読み込まれた暗号化されたポリシデータの復号する。また、Proxyサーバ２０から送信された新たに更新すべきポリシデータを暗号化し、ポリシデータベース６３に保存する。

【００５７】ポリシキャッシュ部６４７は、ポリシデータを一時的にキャッシュしておくモジュールである。復号用共通鍵ポリシ判定部６４４は、ユーザ・Clientマシン認証部６４２にキャッシュされたユーザ情報とポリシキャッシュ部６４７にキャッシュされたポリシデータをもとに復号用共通鍵をViewer６０に送信するかどうか判定する。

【００５８】図２１は機密ファイルリスト及びアクセスポリシ管理部に保管されたアクセスポリシデータテーブルの構成図である。テーブル２１Ａは、Webサーバ１１に格納されている機密ファイルのＵＲＬ２１０１と、各機密ファイルごとにアクセス可能なユーザの識別番号２１０２およびこのテーブル２１Ａのポリシバージョン２１０３を設定したものである。またテーブル２１Ｂは、機密ファイルにアクセス可能なユーザのユーザＩＤ２１０５とパスワード２１０６および割り振られた識別番号２１０４をリストアップしたものである。

【００５９】次に、フローチャートを用いて本実施形態における各モジュール間の処理の流れや関連を説明する。図１４は、Proxyサーバ２０における処理のフローチャートを示したものである。Proxyサーバ２０は、Client１４からアクセス要求を受信すると（ステップ１４００）、Proxyサーバ初期ルーチンに移る（ステップ１４０１）。このルーチンは、Client１４がWebサーバ１１上の機密ファイル５０または非機密ファイル５１にアクセスする為にProxyサーバ２０にアクセスしているのか、ポリシ管理モジュール６４より、ポリシバージョン問い合わせの為にProxyサーバ２０にアクセスしているのかを判定するルーチンである。このProxyサーバ初期ルーチン（ステップ１４０１）については図１６により後述する。

【００６０】このルーチンでWebサーバ１１上の機密ファイル５０または非機密ファイル５１へのアクセスであると判定されると、処理は図１４のステップ１４０２に移り、Proxyサーバ２０は受信データ解析部２０４でアクセス要求ファイルのＵＲＬを調べる。その後、要求ファイルアクセス判定部２０３で機密ファイル５０へのアクセスであるかどうかの判定が行われる（ステップ１４０３）。機密ファイル５０へのアクセスでなければ、要求ファイルアクセス判定部２０３は、Webサーバ１１からアクセス要求ファイルをダウンロードし（ステップ１４０４）、ダウンロードしたファイルに何も処理を施さずにアクセス要求元のClient１４に送信する（ステップ１４０５）。

【００６１】Client１４のアクセス要求ファイルが機密ファイル５０であった場合、Proxyサーバ２０は、Client１４のポリシ管理モジュール６４と通信し、アクセス要求を出しているユーザのユーザＩＤとパスワードを取得する。そして、取得したユーザ情報（ユーザＩＤとパ

スワード）と、機密ファイルリスト及びアクセスポリシ登録部２０２に登録されているユーザ情報と比較照合することにより、ユーザ認証部２０５でユーザの認証を行なう（ステップ１４０６）。この認証の結果、正当なアクセス権限を有するユーザであると認証されなかった場合は、機密ファイル５０へのアクセスを拒否する（ステップ１４０９）。しかし、認証された場合は、ユーザ固有の鍵を暗号用共通鍵データベース２１１から選択し（ステップ１４０７）、Webサーバ１１から機密ファイル５０をダウンロードしたあと（ステップ１４０８）、機密ファイル暗号部２０７で、その鍵を用いて機密ファイル５０をファイル名ごとユーザ固有の暗号用共通鍵で暗号化する（ステップ１４１０）。なお、暗号用共通鍵データベース２１１にユーザ固有の暗号用共通鍵を登録する方法としては、ユーザが機密ファイル閲覧のためにClient１４及びProxyサーバ２０にユーザ登録するときに、Proxyサーバ２０と通信して鍵をClient１４とProxyサーバ２０の両方に作成する方式を採用する。

【００６２】Proxyサーバ２０はポリシ管理モジュール６４と通信し、ポリシ管理モジュール６４のユーザ・Clientマシン認証部６４２にユーザＩＤとパスワードの入力を促すためのダイアログボックスを表示させ、ポリシ管理モジュール６４からProxyサーバ２０に送信されたユーザＩＤとパスワードをもとに、Proxyサーバ２０でユーザ認証を行なう。

【００６３】暗号化された機密ファイル５０は、機密ファイル名変更部２１２においてファイル名が変更され（ステップ１４１１）、機密ファイルキャッシュ部２０９にキャッシュされる。その後、機密ファイルＵＲＬ送信部２１０は、変更したファイル名をもとに、そのファイルをProxyサーバ２０からダウンロードするためのＵＲＬを生成してClient１４に送信する（ステップ１４１２）。そのＵＲＬを受けて、Browser６１は機密ファイル５０をProxyサーバ２０からダウンロードする（ステップ１４１３）。

【００６４】図１６はProxyサーバ２０初期ルーチン（図１４のステップ１４０１）のフローチャートを示したものである。Client１４からのアクセスがポリシ管理モジュール６４からのポリシバージョン問い合わせのアクセスであるかどうか判定する（ステップ１６０１）。この判定法としては、例えば問い合わせのアクセスの際には、Proxyサーバ２０に送信するデータのヘッダに、明示的に特定のビット列を挿入し、このビット列を検出する方法等がある。このアクセスがポリシバージョン問い合わせのアクセスでなかった場合、Webサーバ１１へのアクセス要求であるので、図１４のProxyサーバ処理のステップ１４０２に戻る（ステップ１６０５）。

【００６５】ポリシバージョン問い合わせのアクセスであった場合、問い合わせのアクセスの際にClient１４より送信されてきたClient１４内のポリシデータのバージョンデータを用いて、問い合わせ元のClient１４のポリシバージョンとProxyサーバ２０のポリシバージョンを比較する（ステップ１６０２）。ポリシバージョンが等しかった場合、ポリシ管理モジュール６４にポリシのバージョンが等しいことを通知し（ステップ１６０６）、処理を終了する。ポリシバージョンが等しくなかった場合、Client１４のポリシデータベース６３を更新する必要があるので、Proxyサーバ２０のポリシデータをポリシ管理モジュール６４に送信する（ステップ１６０４）。

【００６６】これにより、ポリシデータベース６３内のポリシデータ、すなわちアクセス権限を判定するためのデータはProxyサーバ２０内で管理されている最新のものに更新される。

【００６７】図１７は、Webサーバ１１上のファイルを参照するときのClient１４における処理のフローチャートを示したものである。Client１４がProxyサーバ２０から送信されたファイルを受信すると（ステップ１７０１）、Browser６１はファイル名を参照し、機密ファイル５０が受信されたかどうかを判定する（ステップ１７０２）。機密ファイル５０が受信されてない場合、Browser６１はそのファイルを自身の表示機能を用いて表示する（ステップ１７０８）。しかし、受信されてきたファイルが機密ファイル５０であった場合、Browser６１はViewer６０を起動する（ステップ１７０３）。Viewer６０はViewer起動判定部６０１１でハードウェア固有情報６５を調べ（ステップ１７０４）、Viewer内認証用ハードウェア固有情報６０１２と照合し、Viewer６０が特定のClient１４にインストールされていることを確認する。Viewer６０に登録されたViewer内認証用ハードウェア固有情報６０１２と、実際に読み込んだハードウェア固有情報６５が一致しなければ、不正にViewer６０がコピーされてインストールされているものと判断して、Viewer６０を終了する（ステップ１７０９）。一致した場合は、Browser６１からViewer６０に、機密ファイル５０のデータが転送され（ステップ１７０６）、暗号化された機密ファイル５０は暗号化機密ファイルキャッシュ部６０１３にキャッシュされる（ステップ１７０７）。その後、機密ファイル名データ除去部６０１４にてファイル名の除去が行われ（ステップ１７１０）、暗号化機密ファイル復号部６０１５で復号された後（ステップ１７１１）、機密ファイル表示部６０１６に復号された機密ファイル５０が表示される（ステップ１７１２）。

【００６８】Webサーバ１１にある機密ファイル５０をダウンロードする際、Proxyサーバ２０におけるユーザ認証のために、ポリシ管理モジュール６４がダイアログボックスを生成し、ユーザにユーザＩＤとパスワードの入力を要求するが、その入力値をもとに、ポリシ管理モジュール６４はClient１４にある共通鍵データベース６２より、対応するユーザ固有の共通鍵を検索し、それを

Viewer６０のViewer内復号用共通鍵キャッシュ部６０１７に転送する。ステップ７１１で復号に使用される共通鍵は、この共通鍵キャッシュ部６０１７にキャッシュされた共通鍵である。

【００６９】図１９は、２次記憶装置６７に保存された機密ファイル５０を参照するときのClient１４における処理を示したフローチャートである。ユーザが２次記憶装置６７に保存された機密ファイル５０にアクセスしたとき、まずViewer６０が起動される（ステップ１９０１）。Viewer６０はポリシ管理モュール６４を起動し、アクセスしようとしている機密ファイル名をポリシ管理モジュール６４に送信する（ステップ１９０２）。ポリシ管理モジュール６４はユーザ・Clientマシン認証部６４２にてユーザＩＤとパスワードの入力をユーザに要求し、同時にClientマシンのハードウェア固有情報６５にアクセスして、認証用ハードウェア固有情報６４８を用いてマシン認証を行なう（ステップ１９０３）。

【００７０】ポリシ管理モジュール６４は、Proxyサーバ２０にユーザＩＤとパスワード、及びClient１４のポリシのバージョンデータを安全な方法で送信し、ポリシバージョンの問い合わせをする。そして、ポリシ管理モジュール６４は、Proxyサーバ２０でのユーザ・Clientマシン認証の結果及びポリシバージョン問い合わせに対する応答を待つ（ステップ１９０４）。Proxyサーバ２０におけるユーザ・Client認証が否定されたか、もしくは通信の失敗が原因でProxyサーバ２０からの応答がなかった場合、ポリシ管理モジュール６４はViewer６０に応答なしの通知を行なう（ステップ１９０９）。これにより、Viewer６０は機密ファイル５０を表示しない（ステップ１９１０）。

【００７１】Proxyサーバ２０からの応答があり、かつその応答の内容としてポリシバージョンが等しくなかった場合には、Proxyサーバ２０から最新のポリシデータが送信され、そのデータをもとにポリシデータベース６３を更新する（ステップ１９０６，１９０７）。バージョンが等しければ、Client１４のポリシデータはそのままにしておく。復号用共通鍵ポリシ判定部６４４は、バージョンが最新のポリシデータを用いて、ユーザＩＤとアクセス対象の機密ファイル名から機密ファイル５０へのアクセスが可能かどうか判定する（ステップ１９０８、１９１１）。判定結果が不可の場合、復号用共通鍵ポリシ判定部６４４はViewer６０に機密ファイル５０へのアクセス拒否エラーを返す（ステップ１９１５）。そのエラーを受けて、Viewer６０は暗号化された機密ファイル５０の復号処理行なわずにエラーを機密ファイル表示部６０１６に表示し、処理を終了する（ステップ１９１６）。

【００７２】また、ポリシ判定結果が可の場合、復号用共通鍵ポリシ判定部６４４は、ユーザに固有の復号用共通鍵を復号用共通鍵データベース６２から検索し、その復号用共通鍵をViewer６０に送信する（ステップ１９１２）。Viewer６０はファイル名を削除の後、ユーザ固有の復号用共通鍵を用いて機密ファイル５０を復号し（ステップ１９１３）、そのデータをViewer６０の機密ファイル表示部６０１６で表示する（ステップ１９１４）。

【００７３】以上のように、この第２の実施形態の情報提供システムは、Webサーバ１１とClient１４との間にProxyサーバ２０を介在させ、このProxyサーバ２０において、Client１４からWebサーバ１１上の機密ファイル５０へのアクセス要求にしたがって、Client１４内のポリシ管理モジュール６４と通信してユーザ及びClientマシンの認証を行い、予め登録されたユーザからのアクセス要求であった場合には、要求された機密ファイル５０をWebサーバ１１からダウンロードし、その機密ファイル５０を要求元のユーザに対応した暗号化のための共通鍵を用いてファイル名ごと暗号化し、ファイル名を変更し、その変更された機密ファイルをClient１４に転送するように構成したものである。

【００７４】これにより、既存のWebサーバ１１の設定を変更することなく、機密ファイル５０に対しユーザごとのアクセス権限を設定でき、その機密ファイル５０を安全にダウンロードできると共に、その機密ファイル５０をClient１４内に安全に保管することができる。また、ユーザごとに機密ファイル５０へのアクセス権限を設定しているので、機密ファイル５０のダウンロードの際に盗聴されても、機密ファイル５０へのアクセス権限のないユーザはそれを閲覧することができない。また、それぞれの機密ファイル５０のアクセス権限の認証は動的に適用され、Proxyサーバ２０でアクセス権限を変更した場合、その変更時点から、アクセス権限はClient１４内に保存してある機密ファイル５０にも適用される。従って、例えば人事部に属していたClient１４のユーザＡが人事異動により、営業部に配置転換された場合には、Proxyサーバ２０内の人事部員以外には機密である人事情報ファイルのアクセス権限リストからユーザＡを削除することにより、ユーザＡが使用しているClient１４内のポリシデータベース６３に対してもその変更内容が図１６のステップ１６０１～１６０４の処理で反映され、ユーザＡは人事異動前と同じClient１４マシンを使用していたとしても機密の人事情報の閲覧は不可能になる。さらに、機密ファイル５０を予め暗号化して、Webサーバ１１に登録しておく必要がないので、Webサーバ１１で動的に生成される機密ファイル５０の管理も可能である。

【００７５】また、Client１４においては、機密ファイル５０を表示するために専用に設けたViewer６０が不正にインストールされたものである場合には、このViewer６０を閉じ、機密ファイルを表示させないようにしているため、不正インストールなどの不正行為に対しても有効に対処し、機密ファイル５０の漏洩を防止することが

できる。

【００７６】また、２次記憶装置６７に保管された機密ファイル５０にアクセスする場合には、Proxyサーバ２０にその都度アクセス権限のバージョンを問い合わせ、最新のアクセス権限判定用の情報でアクセス権限を認証しているため、２次記憶装置６７に保管された機密ファイル５０を、アクセス権限を取り消された者による不正アクセス行為から防衛することができる。なお、アクセス権限のバージョン問い合わせ処理は、２次記憶装置６７をアクセスする都度行なっているが、機密ファイル５０の機密度が低いものである場合には所定時間間隔おきにするなど、問い合わせ回数を少なくするようにしてもよい。これにより、ネットワークのトラフィックを少なくすることに貢献することができる。

【００７７】なお、第２の実施形態においては、ハードコピー禁止モジュールを設けていないが、第１の実施形態と同様に設けることができる。また、機密ファイルを暗号化または復号する際の暗号鍵および復号鍵は、Client１４の装置自身に固有の情報（ＭＡＣアドレス、ＩＰアドレス、ＣＰＵ製造番号など）を元に生成した鍵情報、またはユーザ自身の機密情報（例えばクレジット番号など）から生成した鍵情報を用いてもよい。

【００７８】次に、本発明の第３の実施形態を詳細に説明する。図２２は、本発明の第３の実施形態を示す全体構成図である。この実施形態のシステムは、地図データや写真等の画像データ、新聞・雑誌の記事といったコンテンツ２２０７を保管するWebサーバであるコンテンツサーバ２２０２と、利用者のユーザＩＤやパスワードを用いたアクセス認証、アクセスログの管理、及びコンテンツ配信時にコンテンツデータが盗まれないように暗号化処理を施すコンテンツ配信プロキシ２２０３、及びコンテンツを閲覧するための専用ビューア２２０６ａ～２２０６ｎをそれぞれインストールしたクライアント２２０５ａ～２２０５ｎから構成されている。コンテンツ配信会社２２０１はコンテンツサーバ２２０２、及びコンテンツ配信プロキシ２２０３を管理し、アクセスログを集計して、利用者にダウンロードしたコンテンツに対する料金を請求する。コンテンツ配信を希望する利用者はインターネット２２０４経由で専用ビューア２２０６ａ～２２０６ｎを用いてコンテンツ２２０７をダウンロードする。コンテンツサーバ２２０２にアクセスするためには、必ずコンテンツ配信プロキシ２２０３を経由しなければならない。従って，外部からコンテンツサーバ２２０２への直接的な不正アクセスを防ぐことができる。

【００７９】次に、本発明の第３の実施形態における各構成要素の内部構成、ならびに各構成要素とその構成要素間の処理について説明する。図２３は，本発明の第３の実施形態におけるクライアント構成図である。クライアント２２０５（２２０５ａ～２２０５ｎ）は，専用ビューア２２０６、ユーザ固有鍵ＤＢ２２０５１、クライアント固有データ２２０５３、及び２次記憶装置２２０５２から成る。クライアント固有データ２２０５３として、ＩＣカード内の改竄不可能なデータや特別なハードウェア内のデータ、ＣＰＵに割り当てられたデータ等を用いることができる。

【００８０】専用ビューア２２０６の詳細な説明をする。専用ビューア２２０６は表示部２２０６６、ハードコピー禁止モジュール２２０６７、復号部２２０６３、復号データキャッシュ部２２０６４、暗号・復号化部２２０６５、鍵検索部２２０６１、及び鍵生成部２２０６２から成る。表示部２２０６６はコンテンツを展開して表示する部分である。復号部２２０６３はコンテンツ配信プロキシ２２０３から送信された暗号化されたコンテンツを、鍵検索部２２０６１でユーザ固有鍵ＤＢ２２０５１から検索されたユーザ固有の鍵で復号する部分である。鍵生成部２２０６２は、専用ビューア２２０６の起動時に読み込んだクライアント固有データ２２０５３を元に、コンテンツ保存時に暗号化・復号化するためのクライアント固有の鍵を生成する。鍵検索部２２０６１は、ユーザＩＤ・パスワード情報を元に、ユーザ固有鍵ＤＢ２２０５１から検索してユーザ固有の鍵を抽出する。ユーザＩＤ・パスワード情報は、専用ビューア２２０６に予め登録する、もしくは専用ビューア２２０６を用いてコンテンツ配信プロキシ２２０３へアクセスする際や２次記憶装置２２０５２内に保存された暗号化されたコンテンツにアクセスする際にダイアログを表示して、利用者に入力させるなどの方法で取得する。ユーザ固有鍵ＤＢ２２０５１は、各利用者固有の鍵を管理する部分であり、利用者の鍵は利用者のパスワードを鍵として用いて暗号化する等の処置を施してクライアント２２０５内に安全に保管される。ＩＣカードや別のハードウェア等に保存する方法でもよい。

【００８１】暗号・復号化部２２０６５は鍵生成部２２０６２、及び鍵検索部２２０６１からそれぞれ、クライアント固有の鍵及び利用者固有の鍵を受け取り、その２つの鍵を用いてコンテンツを暗号化、もしくは復号化する。ハードコピー禁止モジュール２２０６７は、キャプチャツールがハードコピーをする際に使用するＯＳのシステムコールをフックして禁止すること、及びハードコピーを撮るためのキーを押下した際に発行されるシステム内のメッセージをフックしてデータのコピー先メモリを使用禁止することにより、表示されている画面のハードコピーを禁止するモジュールである。このモジュールにより、利用者がディスプレイ画面にコンテンツを表示し、そのハードコピーを採取して二次配布することを防止する。

【００８２】図２４は本実施形態におけるコンテンツ配信プロキシ２２０３の構成図である。コンテンツ配信プロキシ２２０３はプロキシサーバ２２０３１、管理アプリケーション２２０３２、ユーザ情報・固有鍵ＤＢ２２

０３３及びログデータ保存部２２０３４から成る。ユーザ情報・固有鍵ＤＢ２２０３３はコンテンツにアクセス可能な利用者のユーザＩＤ、パスワード、鍵データ及びアクセス可能なコンテンツのＵＲＬ情報を格納するデータベースであり、管理アプリケーション２２０３２によりユーザ情報・固有鍵ＤＢ２２０３３への設定情報の登録・削除・変更が行われる。プロキシサーバ２２０３１は、クライアント２２０５のコンテンツサーバ２２０２へのアクセスを中継して処理するプログラムであり、コンテンツへのアクセスログをログデータ保存部２２０３４に書き込む。

【００８３】プロキシサーバ２２０３１の詳細説明に移る。プロキシサーバ２２０３１はコンテンツキャッシュ部２２０３５、ユーザ認証部２２０３６、受信データ解析部２２０３７、及びコンテンツ暗号化部２２０３８から成る。クライアント２２０５から送信されるアクセス要求は、アクセス要求コンテンツのＵＲＬ、ユーザＩＤ及びパスワードで構成されており、プロキシサーバ２２０３１は受信したアクセス要求を受信データ解析部２２０３７で解析する。受信データ解析部２２０３７で取得したユーザ情報、及びアクセス要求コンテンツのＵＲＬを元に、ユーザ情報・固有鍵ＤＢ２２０３３を検索し、ユーザ認証、及びコンテンツへのアクセスが可能かどうか判定を行なう。認証が成功すると、コンテンツサーバ２２０２にクライアント２２０５からのリクエストを送信し、ダウンロードしたコンテンツデータを、ユーザ情報・固有鍵ＤＢ２２０３３から検索した利用者固有の鍵で暗号化してクライアント２２０５に送信する。

【００８４】図２５は本実施形態におけるコンテンツ配信プロキシ２２０３で保存されるコンテンツアクセスログデータの概要構成図である。これはコンテンツ配信プロキシ２２０３のログデータ保存部２２０３４に記録されるデータエントリーであり、トランザクション番号２５０１、ユーザＩＤ２５０２、アクセス日時２５０３、アクセスコンテンツＵＲＬ２５０４、課金フラグ２５０５で構成されている。トランザクション番号２５０１はテーブルのキーとなる値で、クライアント２２０５からコンテンツ２２０７へのアクセスごとに割り振られる。アクセスコンテンツＵＲＬ２５０４は、利用者がアクセスしたコンテンツ２２０７のＵＲＬである。課金フラグ２５０５は、そのトランザクションに対して課金するかどうかを示すフラグで、例えば同じ利用者による同一コンテンツの２回目以降のアクセスに対しては課金しないサービスの場合等に利用する。

【００８５】図２６は本実施形態におけるユーザ情報・固有鍵ＤＢ２２０３３に記録されたアクセス可能な利用者のユーザ情報を示す概要構成図である。このテーブルの各エントリーはユーザＩＤ２６０１、パスワード２６０２、サービス登録日２６０３、サービス利用期限日２６０４、固有鍵データ２６０５、及びアクセス可能コンテンツＵＲＬ２６０６で構成されている。サービス登録日２６０３は、利用者がWeb経由でコンテンツ配信サービスに登録した日付であり、サービス利用期限日２６０４は、利用者の配信サービス授受可能な期日を表す。固有鍵データ２６０５はユーザに固有の鍵データを登録しておく項目である。また、アクセス可能コンテンツＵＲＬ２６０６はユーザがアクセス可能なコンテンツのＵＲＬのリスト２６０７へのポインタが登録されており、利用者により選択された配信サービスを受けたいコンテンツに対応している。上記のエントリーは登録された利用者ごとに用意されており、コンテンツ配信プロキシ２２０３の管理アプリケーション２２０３２で登録・削除・変更を行なう。

【００８６】図２７は、本実施形態におけるコンテンツ配信サービスにおける全体の流れを時系列で示した図である。この図に従って、利用者のコンテンツ配信サービス依頼からサービスの処理、サービス料金の支払いまでの一連の流れについて説明する。利用者はコンテンツ配信会社２２０１のコンテンツ配信サービスのサイトにアクセスして、コンテンツの表示に必要な専用ビューア２２０６をダウンロードしてクライアント２２０５にインストールする（ステップ２７０１）。利用者は専用ビューア２２０６を用いてWeb経由でコンテンツ配信を依頼する（ステップ２７０２）。コンテンツ配信会社２２０１のコンテンツ配信プロキシ２２０３の管理アプリケーション２２０３２は、利用者のユーザＩＤ、パスワード、アクセス可能なコンテンツＵＲＬ等の設定情報をユーザ情報・固有鍵ＤＢ２２０３３に登録する（ステップ２７０３）。また、この際に生成されるコンテンツ配信の際に使用するユーザに固有の鍵データもユーザ情報・固有鍵ＤＢ２２０３３の固有鍵データエントリ２６０５に登録する。そして、この登録した固有鍵を利用者に通信を暗号化するなど、安全な方法で配信する（ステップ２７０４）。

【００８７】次に配信サービスが行われるが、その流れについて説明する。まず、利用者は専用ビューア２２０６を用いてコンテンツ２２０７にアクセスする（ステップ２７０５）。コンテンツ配信会社２２０１はコンテンツ２２０７へのアクセスに対してアクセスログを採取することで利用者に対する課金処理を行なう（ステップ２７０６）。そして、アクセス要求されたコンテンツを利用者に配信する（ステップ２７０７）。この流れを利用者のコンテンツ２２０７へのアクセスごとに繰り返す。最後に、コンテンツ配信会社２２０１は予め定めたれた期間末に、利用者ごとに決済を行い（ステップ２７０８）、クレジットカード会社経由で利用者にコンテンツ使用料を請求する（ステップ２７０９）。利用者は請求に応じてコンテンツ使用料の支払いを行なう（ステップ２７１０）。

【００８８】図２８は、コンテンツ２２０７をダウンロ

ードして専用ビューア２２０６で閲覧する際のフローチャートである。以下、フローチャートに従って処理の流れを説明する。利用者は、クライアント２２０５にインストールされた専用ビューア２２０６を使用して、コンテンツ配信プロキシ２２０３にアクセスする（ステップ２８０１）。アクセスの方法として、利用者は専用ビューア２２０６のインターフェイス（後述の図３０参照）にあるコンテンツのＵＲＬを入力するエディットボックス３００１に、閲覧したいコンテンツのＵＲＬを入力してアクセス要求を送信する。コンテンツのＵＲＬを送信する際に、専用ビューア２２０６に予め登録されているか、もしくはダイアログボックスを表示してユーザにより入力されたユーザＩＤとパスワードも、コンテンツＵＲＬと共にコンテンツ配信プロキシ２２０３に送信する（ステップ２８０２）。

【００８９】コンテンツ配信プロキシ２２０３は専用ビューア２２０６から送信されたリクエストを解析して、送信されたユーザＩＤ、パスワード、及びコンテンツのＵＲＬを元にユーザ情報・固有鍵ＤＢ２２０３３に検索をかけ、ユーザ認証、及びコンテンツアクセス許可判定を行なう（ステップ２８０３）。認証・アクセス許可判定が成功しない場合、プロキシサーバ２２０３１はクライアント２２０５にコンテンツ利用不可を表示するデータを送信し（ステップ２８０６）、処理を終了する。成功した場合、プロキシサーバ２２０３１はコンテンツサーバ２２０２からコンテンツをダウンロードして、ユーザ情報・固有鍵ＤＢ２２０３３に登録された固有鍵を使用して暗号化を行い（ステップ２８０４）、要求元のクライアント２２０５の専用ビューア２２０６に送信する。専用ビューア２２０６は、暗号化されたコンテンツを、ユーザ固有鍵ＤＢ２２０５１で検索した固有鍵を使用して復号表示する（ステップ２８０５）。

【００９０】図２９はクライアント２２０５にコンテンツデータを保存する際の、専用ビューアが行なう処理のフローチャートを示したものである。以下、このフローチャートに従って、処理の流れを詳細に説明する。専用ビューア２２０６は起動時にクライアント固有データ２２０５３をアプリケーション内に取得する（ステップ２９０１）。そして、取得したクライアント固有データ２２０５３を元に、鍵生成部２２０６２においてクライアント固有の鍵を生成する（ステップ２９０２）。次に、専用ビューア２２０６は、コンテンツをダウンロードする際に使用するためのユーザＩＤとパスワードを、ダイアログボックスを表示して利用者に入力してもらうか、もしくは予め専用ビューア２２０６に登録されているのであればそれを読み取る（ステップ２９０３）。そして、受け取ったユーザ情報をもとに、専用ビューア２２０６内の鍵検索部２２０６１において、利用者固有の鍵を検索して抽出する（ステップ２９０４）。この生成・抽出された２つの鍵を利用して、専用ビューア２２０６内の暗号・復号化部２２０６５においてコンテンツデータを暗号化する（ステップ２９０５）。最後に、暗号化したコンテンツデータを２次記憶装置２２０５２に保存する（ステップ２９０６）。２次記憶装置２２０５２に保存されたコンテンツデータを復号表示する際にも、同様の手順で行なう。このように、コンテンツを暗号・復号化するための２つの鍵が、それぞれクライアント２２０５、及び利用者に固有であるため、もし、保存されたコンテンツデータを、専用ビューア２２０６のインストールされた他のクライアントにコピーして表示しようとしてもできない。従って、配信されたコンテンツのアクセス権を保持する利用者による２次配信を防ぐことができる。

【００９１】図３１は、専用ビューア２２０６を使用してデジタルコンテンツ配信サービスに登録する際のインターフェイスの移り変わりを表した図である。利用者は、まずコンテンツ配信会社２２０８のサイトからダウンロードしてきた専用ビューア２２０６を使用し、デジタルコンテンツ配信登録ページ３１０１にアクセスする。デジタルコンテンツ配信登録ページ３１０１は、氏名、性別、住所、メールアドレス、クレジットカード番号等の個人情報、配信サービスで利用する利用者希望のユーザＩＤ・パスワード、及び配信サービスを受けたいコンテンツ項目を入力するフォームで構成されている。利用者はこれらのフォームに記入して「ＯＫ」ボタンを押す。また、フォームの入力を白紙に戻したい場合は「取消」ボタンを押す。「ＯＫ」ボタンを押すと、入力情報確認のページ３１０２が表示される。このページ３１０２で、利用者は先に入力した情報を確認する。入力情報が正しければ「送信」ボタンを押す。入力情報が正しくない、もしくはコンテンツ配信サービスの登録を中止する場合には、それぞれ「戻る」もしくは「中止」ボタンを押す。「送信」ボタンを押すと、入力情報がコンテンツ配信プロキシ２２０３に送信される。そして、管理アプリケーション２２０３２により利用者に固有の鍵が生成され、ユーザＩＤやパスワード、ユーザ情報と共にユーザ情報・固有鍵ＤＢ２２０３３に登録される。その後、固有鍵データがコンテンツ配信プロキシ２２０３よりクライアント２２０５内の専用ビューア２２０６に送信される。その際、図３２に示すようにデータの送信状況を示す画面３１０３がクライアント２２０５に表示される。利用者の固有鍵の送信が完了すると、図３２に示す登録完了ページ３１０４が表示される。このページ３１０４には登録された利用者のユーザＩＤ情報が表示される。パスワード情報はメールにより別途利用者に送信される。これにより、利用者は登録されたパスワード情報の確認も行なう。

【００９２】図３３は本発明の第４の実施形態を示した全体構成図である。コンテンツ配信サービスは、クライアント３３０３、コンテンツ配信会社３３０１、クレジ

ットカード会社３３０２の３者間で行われる。コンテンツ配信会社３３０１はコンテンツ３３０６と、コンテンツ３３０６を格納するWebサーバであるコンテンツサーバ３３０５を管理している。また、コンテンツ配信ブロキシ３３０７はクレジットカード会社３３０２で管理されており、クライアント３３０３には専用ビューア３３０８がインストールされている。各関係者はインターネット３３０４経由でそれぞれ通信を行なう。コンテンツサーバ３３０５にはコンテンツ配信ブロキシ３３０７しかアクセスできず、かつ通信は安全なものとする。例えば両者を専用線で接続、あるいはＳＳＬクライアント認証通信等の方法でコンテンツサーバ３３０５はコンテンツ配信ブロキシ３３０７を認証したうえで通信を行なう。本実施形態ではコンテンツサーバ３３０５とコンテンツ配信ブロキシ３３０７はＳＳＬクライアント認証方式で通信を行なうものとする。

【００９３】図３４は本実施形態におけるクライアント３３０３の構成図を示したものである。クライアント３３０３は、２次記憶装置３４０１、クレジットカードデータ３４０２、専用ビューア３３０８から成る。クレジットカードデータ３４０２はクレジットカードの番号情報で、クライアント３３０３に平文のままで保存されているか、パスワードとして利用者が専用ビューア３３０８に入力するものとする。専用ビューア３３０８は、復号データキャッシュ部３４０３、表示部３４０４、ハードコピー禁止モジュール３４０５、暗号・復号化部３４０６、鍵生成部３４０７、及びハッシュ生成部３４０８で構成される。コンテンツ配信ブロキシ３３０７より送信されたコンテンツデータを暗号・復号するための鍵は、ハッシュ生成部３４０８でクレジットカードデータ３４０２のハッシュ値を計算し、そのハッシュ値を元に鍵生成部３４０７で生成され、一時的に格納される。この鍵生成は専用ビューア３３０８の起動ごとに行われる。鍵生成部３４０７に格納された鍵は、専用ビューア３３０８のプロセスが終了する際に消去される。暗号・復号化部３４０６はキャッシュされた鍵を元にコンテンツデータを暗号・復号化するモジュールである。復号データキャッシュ部３４０３、表示部３４０４、及びハードコピー禁止モジュール３４０５については第１の実施形態と同様の構成および機能である。

【００９４】図３５は、本実施形態におけるコンテンツ配信ブロキシ３３０７の構成図を示したものである。コンテンツ配信ブロキシ３３０７は、ブロキシサーバ３５０１１、管理アプリケーション３５０２、ユーザ情報・固有鍵ＤＢ３５０３、及びログデータ保存部３５０４より構成される。ユーザ情報・固有鍵ＤＢ３５０３はコンテンツにアクセス可能な利用者のクレジットカード番号、クレジットカード番号のハッシュ値、利用者固有の鍵データ及びアクセス可能なコンテンツのＵＲＬ情報を格納するデータベースであり、管理アプリケーション３５０２により設定情報の登録・削除・変更が行われる。ブロキシサーバ３５０１はクライアント３３０３のコンテンツサーバ３３０５へのアクセスを中継して処理するプログラムであり、コンテンツ３３０６へのアクセスログをログデータ保存部３５０４に書き込む。第３の実施形態と違って、本実施形態ではユーザＩＤとパスワードによるユーザ認証の代わりに、クレジットカードデータのハッシュ値による利用者のユーザ認証を行なう。これは、コンテンツ配信ブロキシ３３０７を管理しているのがクレジットカード会社であるため、クレジットカード番号と利用者を１対１に対応づけることができ、クレジットカード番号による利用者の識別の方が課金処理の際に便利だからである。また、管理アプリケーション３５０２は利用者ごとにコンテンツを暗号化するための鍵の生成するが、この鍵は専用ビューア３３０８内で生成する方法と同じ方法、すなわちクレジットカードデータ３４０２よりハッシュ値を求め、その値を元に鍵を生成する方法で生成される。専用ビューア３３０８からコンテンツ配信ブロキシ３３０７にユーザ認証のためにクレジットカード番号のハッシュ値を送る際には、このハッシュ値がインターネット３３０４上で盗まれないように暗号化処理を行っておく必要がある。

【００９５】次に、ブロキシサーバ３５０１の詳細説明を行なう。ブロキシサーバ３５０１は、ＳＳＬ通信制御部３５０５、ユーザ認証部３５０６、受信データ解析部３５０７、コンテンツ暗号化部３５０８、及び通信制御部３５０９で構成される。ＳＳＬ通信制御部３５０５は、コンテンツサーバ３３０５とコンテンツ配信ブロキシ３３０７の通信として、ＳＳＬによるクライアント認証通信を実現するためのモジュールである。これにより、コンテンツサーバ３３０５にはコンテンツ配信ブロキシ経由でしかアクセスできず、また、通信盗聴者によるコンテンツサーバ３３０５からコンテンツ配信ブロキシ３３０７への通信時のコンテンツデータの漏洩を防ぐ。受信データ解析部３５０７、ユーザ認証部３５０６及びコンテンツ暗号化部３５０８は第３の実施形態と同様の構成及び機能である。通信制御部３５０９はブロキシサーバ３５０１とクライアント３３０３間の通信を司る部分である。

【００９６】図３６はコンテンツ配信サービス全体の流れを時系列で表した図である。以下、この図に従ってサービス全体の流れを説明する。コンテンツ配信会社３３０１は予めクレジットカード会社３３０２にコンテンツ配信サービスにおける課金処理を依頼し、クレジットカード会社３３０２とコンテンツ配信会社３３０１の双方は、課金サービスについての契約を交わす（ステップ３６０１）。契約が成立すると、クレジットカード会社３３０２はコンテンツ配信ブロキシ３３０７を設置し、コンテンツ配信サービスを開始する。コンテンツ配信サービスを受けたい利用者は、クレジットカード会社３３０

２とカード使用契約を行い、クレジットカードを取得する（ステップ３６０２）。コンテンツ配信サービスを受けるために、利用者はコンテンツ配信会社３３０１のサイトにアクセスして専用ビューア３３０８をダウンロードし、専用ビューア３３０８を使用してコンテンツ配信サービスを実施する（ステップ３６０３）。そして一定期間ごとに決済を行い（ステップ３６０４）、コンテンツ料金を利用者に代わってコンテンツ配信会社３３０１に立て替える（ステップ３６０５）。そして、クレジットカード会社３３０２は利用者にコンテンツ料金の請求を行い（ステップ３６０６）、利用者はその請求に対してコンテンツ料金の支払いを行なう（ステップ３６０７）。

【００９７】図３７は、コンテンツ３３０６をダウンロードして専用ビューア３３０８で閲覧する際のフローチャートを示している。まず、利用者は専用ビューア３３０８を使用してコンテンツ配信プロキシ３３０７にインターネット３３０４経由でアクセスする（ステップ３７０１）。コンテンツ配信プロキシ３３０７との接続が確立した後、専用ビューア３３０８からコンテンツ配信プロキシ３３０７にクレジットカード番号のハッシュ値が暗号化されて送信される（ステップ３７０２）。プロキシサーバ３５０１でクライアント３３０３からの送信データを解析し、クレジットカードのハッシュ値を元にユーザ認証部３５０６にて利用者のユーザ認証、及びアクセス許可判定が行われる（ステップ３７０３）。ユーザ認証が成功すれば、プロキシサーバ３５０１はコンテンツサーバ３３０５との間でＳＳＬクライアント認証接続を行い（ステップ３７０４）、ＳＳＬクライアント認証成功の後、コンテンツサーバ３３０５からコンテンツ３３０６をダウンロードして暗号化する（ステップ３７０５）。暗号化されたコンテンツ３３０６はクライアント３３０３に送信され、専用ビューア３３０８で暗号化されたコンテンツが復号表示される（ステップ３７０６）。しかし、ユーザ認証が成功しなかった場合には、クライアント３３０３に利用不可のページを表示する（ステップ３７０７）。

【００９８】図３８はクライアント３３０３にコンテンツデータを保存する際の専用ビューア３３０８が行なう処理のフローチャートである。専用ビューア３３０８は起動時にクレジットカードデータ３４０２を取得する（ステップ３８０１）。そして、ハッシュ生成部３４０８においてクレジットカードデータ３４０２のハッシュ値を計算する（ステップ３８０２）。さらに、鍵生成部３４０７においてハッシュ値を元に利用者固有の鍵を生成する（ステップ３８０３）。そして生成された鍵は鍵生成部３４０７にて保管される。コンテンツデータを保存する際に、この生成された鍵を元にコンテンツデータの暗号化を行い（ステップ３８０４）、暗号化されたデータを２次記憶装置３４０１に保存する（ステップ３８０５）。

【００９９】本実施形態が、第３の実施形態と異なる特徴点を挙げると次の通りである。まず、専用ビューアがダウンロードしたコンテンツデータを保存するときに、利用者が他の人に公開することのできないクレジットカード番号を元にコンテンツデータを暗号化する点がある。この方法を採用することにより、悪意ある利用者がダウンロードしたコンテンツを第３者に２次配布するためには、自分自身のクレジットカード番号を公開するという危険を負わなければならない。通常はこのような危険を冒すことは考えられないため、結果的に、第３者に２次配布することを抑制することが可能になる。また、第３の実施形態では、ダウンロードして保存したクライアントでしかコンテンツを利用することができないが、本実施形態では利用者が別のマシンに暗号化保存されたデータをコピーして、パスワード入力もしくはコピー先のマシンの所定の場所にクレジットカードデータを書き込むことで利用することができる。

【０１００】ところで、上記で説明した第１～第４の実施形態において、コンテンツ提供サーバからクライアントに配信するコンテンツは、専用ビューアに表示する可視データであるものと説明したが、本発明で扱うことができる配信データは、書類、新聞、雑誌、写真、絵画等の静止画、映画やテレビ等の動画データだけでなく、音楽または音声として再生可能なデータ、医療機関で扱うカルテ等の医療情報、公共機関が発行する電子化された書類（住民票、印鑑証明書など）、無人の物品引取り所において保管庫から物品等を受取るロッカー鍵に相当する受け取り票などのデータも含まれるものである。また、機械的な動作として再現するための制御データも含まれる。機械的な動作として再現するデータとしては、例えば介護ロボットに掃除、洗濯などの特定の動作をさせるものが考えられる。従って、専用ビューアは可視化データを表示するディスプレイに限定されるものではなく、音声、音楽を再生出力する装置、あるいは機械的な動きに再現する装置を含むものである。

【０１０１】また、いずれの実施形態においても、ユーザはコンテンツサーバから直接にコンテンツ配信サービスを受ける例を示したが、地域別に区分けされた２次配信サービス業者または機関を経由する構成であってもよい。図３９は、その例を示す構成図であり、専用ビューア３９０７を備えたクライアント３９０４ａ～３９０４ｎは地域別に分割された中継地点ａ～ｎの２次配信サービス機関３９０２ａ～３９０２ｎにコンテンツ配信要求をインターネット３９０３を介して行なう。要求を受けた中継地点ａ～ｎの２次配信サービス機関３９０２ａ～３９０２ｎのコンテンツ配信プロキシ３９０６では、要求されたコンテンツがキャッシュされていれば、それを要求元のクライアントに配信する。キャッシュされていなければ、中継サーバ３９０５を介してコンテンツ配信

会社３０９１のコンテンツサーバ３９０３に要求し、取得したコンテンツを要求元のクライアントに配信する。

【０１０２】

【発明の効果】以上説明したように、本発明によれば、既存のWebサーバ上に構築されたデータベース内の機密情報を、既存のWebサーバを改変することなく、かつクライアントコンピュータなどの要求元装置（または端末）のハードウェア構成に依存することなく、一般のページと同様にネットワーク経由でアクセス権限を有する者のみに閲覧可能にすることができる。また、閲覧した機密情報を第３者に漏洩しないように要求元装置内に保存・管理することができる。また、デジタルコンテンツに課金して配信するサービスにおいて、利用者に配信されたデジタルコンテンツが２次配信されることを防ぎ、デジタルコンテンツ配信サービスにおける正当な課金の仕組みを維持し、不正コピーによる配信サービス業における経営基盤の崩壊を防ぐことに貢献することができる。

【図面の簡単な説明】

【図１】本発明における情報提供システムの第１の実施形態を示す全体構成図である。

【図２】図１の実施形態におけるProxyサーバのブロック構成図である。

【図３】図１の実施形態における通信フックモジュールブロック構成図である。

【図４】図１の実施形態における外部Viewerのブロック構成図である。

【図５】図１の実施形態におけるProxyサーバの処理を示すフローチャートである。

【図６】図１の実施形態における通信フックモジュールのデータ送信時における処理を示すフローチャートである。

【図７】図１の実施形態における通信フックモジュールのデータ受信時における処理を示すフローチャートである。

【図８】図１の実施形態における２次記憶装置アクセス制御部の機密ファイルアクセス時の処理を示すフローチャートである。

【図９】図１の実施形態における外部Viewerの受信データ表示処理を示すフローチャートである。

【図１０】本発明の情報提供システムの第２の実施形態を示す全体構成図である。

【図１１】図１０の実施形態におけるClientのブロック構成図である。

【図１２】図１０の実施形態におけるProxyサーバのブロック構成図である。

【図１３】図１０の実施形態におけるClient内のポリシ管理モジュールのブロック構成図である。

【図１４】図１０の実施形態におけるProxyサーバの処理を示すフローチャートである。

【図１５】図１４の続きを示すフローチャートである。

【図１６】図１０の実施形態におけるProxyサーバの初期ルーチンを示すフローチャートである。

【図１７】図１０の実施形態におけるWebサーバ上のファイル参照時のClientにおける処理を示すフローチャートである。

【図１８】図１７の続きを示すフローチャートである。

【図１９】図１０の実施形態における２次記憶装置に保存された機密ファイル参照時のClientにおける処理を示すフローチャートである。

【図２０】図１９の続きを示すフローチャートである。

【図２１】図１０の実施形態における機密ファイルリスト及びアクセスポリシ管理部に保管されたアクセスポリシデータテーブルの構成図である。

【図２２】本発明の第３の実施形態を示す全体構成図である。

【図２３】第３の実施形態におけるクライアント構成図である。

【図２４】第３の実施形態におけるコンテンツ配信ブロキシ構成図である。

【図２５】第３の実施形態においてコンテンツ配信ブロキシで保存されるコンテンツアクセスログデータの概要構成図である。

【図２６】第３の実施形態においてユーザ情報・固有鍵ＤＢに記録されたアクセス可能な利用者のユーザ情報の概要構成図である。

【図２７】第３の実施形態においてコンテンツ配信サービスにおける全体の流れを時系列で示した図である。

【図２８】第３の実施形態においてコンテンツをダウンロードして専用ビューアで閲覧する際のフローチャートである。

【図２９】第３の実施形態においてクライアントにコンテンツデータを保存する際の専用ビューアが行なう処理のフローチャートである。

【図３０】第３の実施形態において専用ビューアインターフェイス図である。

【図３１】第３の実施形態において専用ビューアを使用してデジタルコンテンツ配信サービスに登録する際のインターフェイスの移り変わりを表した図である。

【図３２】図３１の続きを示す図である。

【図３３】本発明の第４の実施形態を示す全体構成図である。

【図３４】第４の実施形態におけるクライアント構成図である。

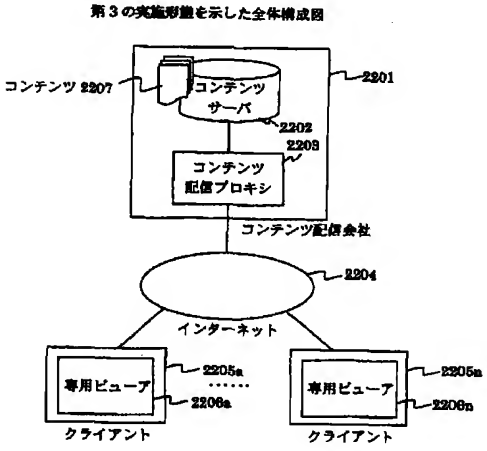
【図３５】第４の実施形態におけるコンテンツ配信ブロキシ構成図である。

【図３６】第４の実施形態におけるコンテンツ配信サービス全体の流れを時系列で示した図である。

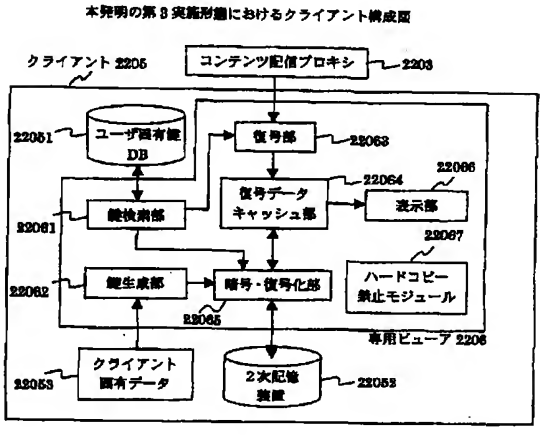
【図３７】第４の実施形態においてコンテンツをダウンロードして専用ビューアで閲覧する際のシステム全体の

フローチャートである。
【図３８】第４の実施形態においてクライアントにコンテンツデータを保存する際の専用ビューアが行なう処理のフローチャートである。
【図３９】中継サーバを介して配信サービスを行なう場合の例を示す全体構成図である。
【図４０】従来システムの構成図である。
【符号の説明】
１１…Webサーバ、１２…ルータ、１３…ネットワーク、１４…Client、１５，６１…Browser、１６…ハードコピー禁止モジュール、１７…２次記憶装置、１８…２次記憶装置アクセス制御部、１９…アクセストークン、２０…Proxyサーバ、２２…機密ファイルＵＲＬ登録部、２３…Client１４マシン識別子データベース、２４…Proxy内受信データ解析部、２５…Clientマシン認証部、２７…機密ファイル識別子付加部、２８…機密ファイル暗号化部、２９…共通鍵データベース、３０…通信フックモジュール、３２…機密ファイル識別子格納部、３３…暗号化ファイル復号部、３４…共通鍵格納部、３５…受信データ解析部、３６…送信データ解析部、３８…Clientマシン識別子付加部、３９…Viewer起動処理部、４０…外部Viewer、４２…機密ファイル表示部、４３…機密ファイルキャッシュ部、４４…機密ファイルアクセス・保存処理部、４５…ハードコピー禁止モジュール起動処理部、４６…２次アクセス制御部起動処理部、４７…外部Viewer起動判定部、５０…機密ファイル、５１…非機密ファイル、６０…Viewer、６２…復号用共通鍵データベース、６５…ハードウェア固有情報、６３…ポリシデータベース、６４…ポリシ管理モジュール、６０１１…Viewer起動判定部、６０１４…機密ファイル名データ除去部、６０１５…暗号化機密ファイル復号部、６０１６…機密ファイル表示部、２０２…機密ファイル＊ファイルリスト及びアクセスポリシ管理部、２０３…要求ファイルアクセス判定部、２０５…ユーザ認証部、２０６…暗号用共通鍵選択部、２０７…機密ファイル暗号部、２１０…機密ファイルＵＲＬ送信部、２１１…暗号用共通鍵データベース、２１２…機密ファイル名変更部、６４４…復号用共通鍵ポリシ判定部、６４６…ポリシ暗号・復号化部、２２０１…コンテンツ配信会社、２２０２…コンテンツサーバ、２２０３…コンテンツ配信プロキシ、２２０４…インターネット、２２０５ａ～２２０５ｎ，２２０５…クライアント、２２０６，２２０６ａ～２２０６ｎ…専用ビューア、２２０７…コンテンツ、２２０５１…ユーザ固有鍵ＤＢ、２２０５２…２次記憶装置、２２０５３…クライアント固有データ、２２０６１…鍵検索部、２２０６２…鍵生成部、２２０６３…復号部、２２０６５…暗号・復号化部、２２０６７…ハードコピー禁止モジュール、２２０３１…プロキシサーバ、２２０３２…管理アプリケーション、２２０３３…ユーザ情報・固有鍵ＤＢ、２２０３４…ログデータ保存部、２２０３６…ユーザ認証部、２２０３７…受信データ解析部、２２０３８…コンテンツ暗号化部、３３０２２…クレジットカード会社、３３０３…クライアント、３３０５…コンテンツサーバ、３３０６…コンテンツ、３３０７…コンテンツ配信プロキシ、３３０８…専用ビューア、３４０１…２次記憶装置、３４０２…クレジットカードデータ、３４０５…ハードコピー禁止モジュール、３４０６…暗号・復号化部、３４０７…鍵生成部、３４０８…ハッシュ生成部、３５０１…プロキシサーバ、３５０２…管理アプリケーション、３５０３…ユーザ情報・固有鍵ＤＢ、３５０４…ログデータ保存部、３５０５…ＳＳＬ通信制御部、３５０６…ユーザ認証部、３５０７…受信データ解析部、３５０８…コンテンツ暗号化部。

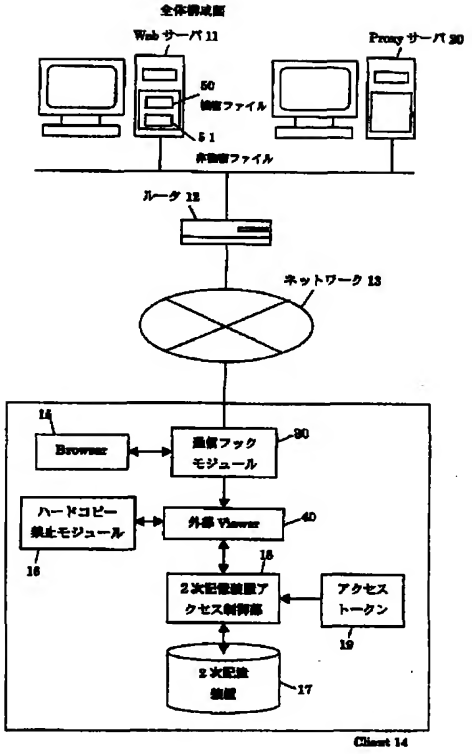
【図２２】



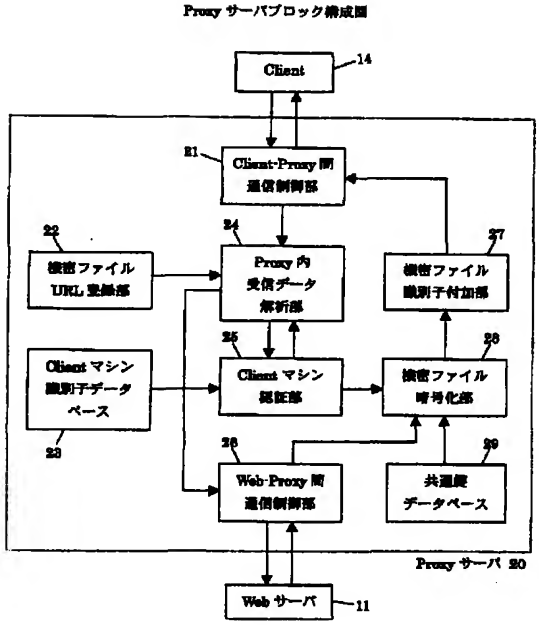
【図２３】



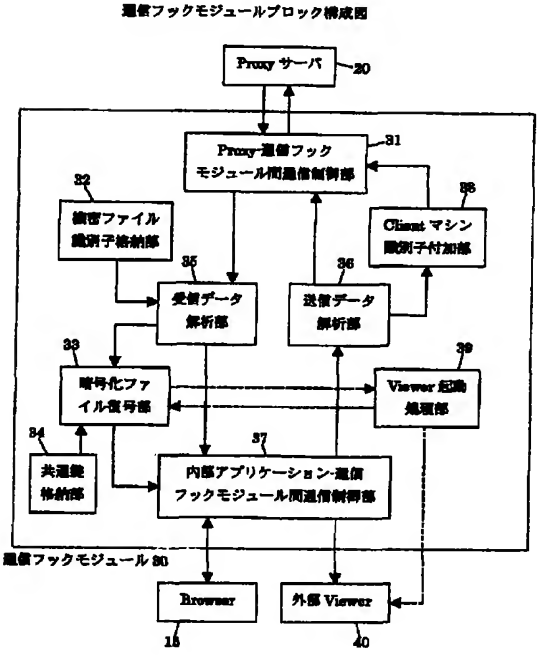
【図１】


全体構成図
Web サーバ 11
Proxy サーバ 20
50
機密ファイル
51
非機密ファイル
ルータ 12
ネットワーク 13
14
Browser
通信フック
モジュール
30
ハードコピー
禁止モジュール
16
外部 Viewer
40
15
2次記憶装置ア
クセス制御部
アクセス
トークン
19
2次記憶
装置
17
Client 14

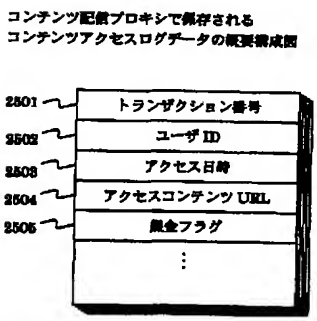
【図２】


Proxy サーバブロック構成図
Client
14
21
Client-Proxy 間
通信制御部
22
機密ファイル
URL 登録部
24
Proxy 内
受信データ
解析部
27
機密ファイル
識別子付加部
Client マシン
識別子データ
ベース
23
25
Client マシン
認証部
28
機密ファイル
暗号化部
26
Web-Proxy 間
通信制御部
29
共通鍵
データベース
Proxy サーバ 20
Web サーバ
11

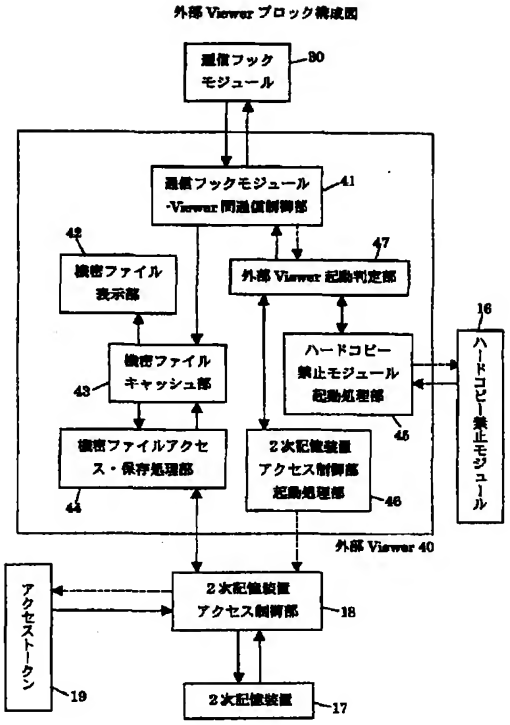
【図３】


通信フックモジュールブロック構成図
Proxy サーバ
20
Proxy-通信フック
モジュール間通信制御部
31
22
機密ファイル
識別子格納部
38
Client マシン
識別子付加部
35
受信データ
解析部
36
送信データ
解析部
33
暗号化ファ
イル復号部
39
Viewer 起動
処理部
34
共通鍵
格納部
37
内部アプリケーション-通信
フックモジュール間通信制御部
通信フックモジュール 30
Browser
外部 Viewer
15
40

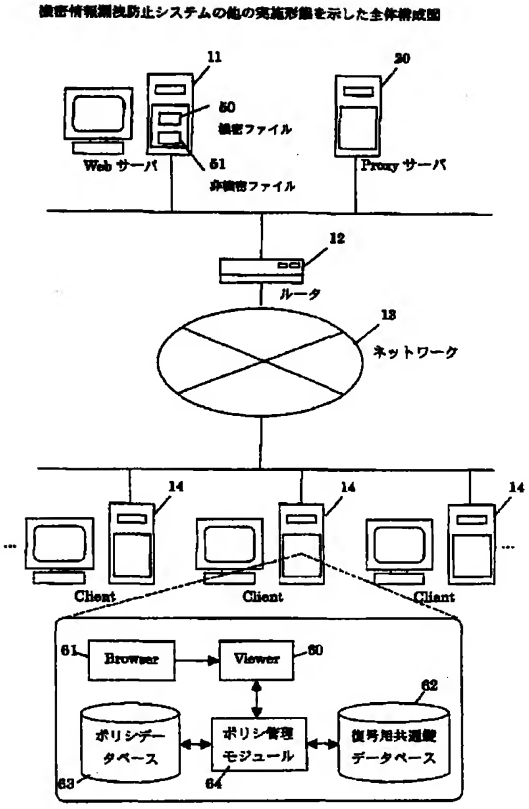
【図２５】


コンテンツ配信プロキシで保存される
コンテンツアクセスログデータの概要構成図
2501
トランザクション番号
2502
ユーザ ID
2503
アクセス日時
2504
アクセスコンテンツ URL
2505
課金フラグ

【図４】



【図１０】



【図２１】

機密ファイルリスト及びアクセスポリシ管理部に保管された
アクセスポリシデータテーブル図

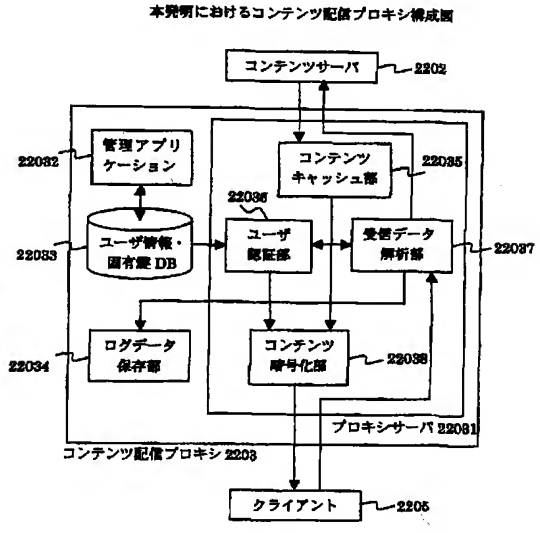
21A

2101 機密ファイル URL	2102 アクセス可能ユーザ	2103 ポリシバージョン
http://www.secure/secret1.html	001,002,003	2000/1/11/14:50
http://www.secure/secret2.html	004,006,	
http://www.secure/secret3.html	002,004,009	
⋮	⋮	

21B

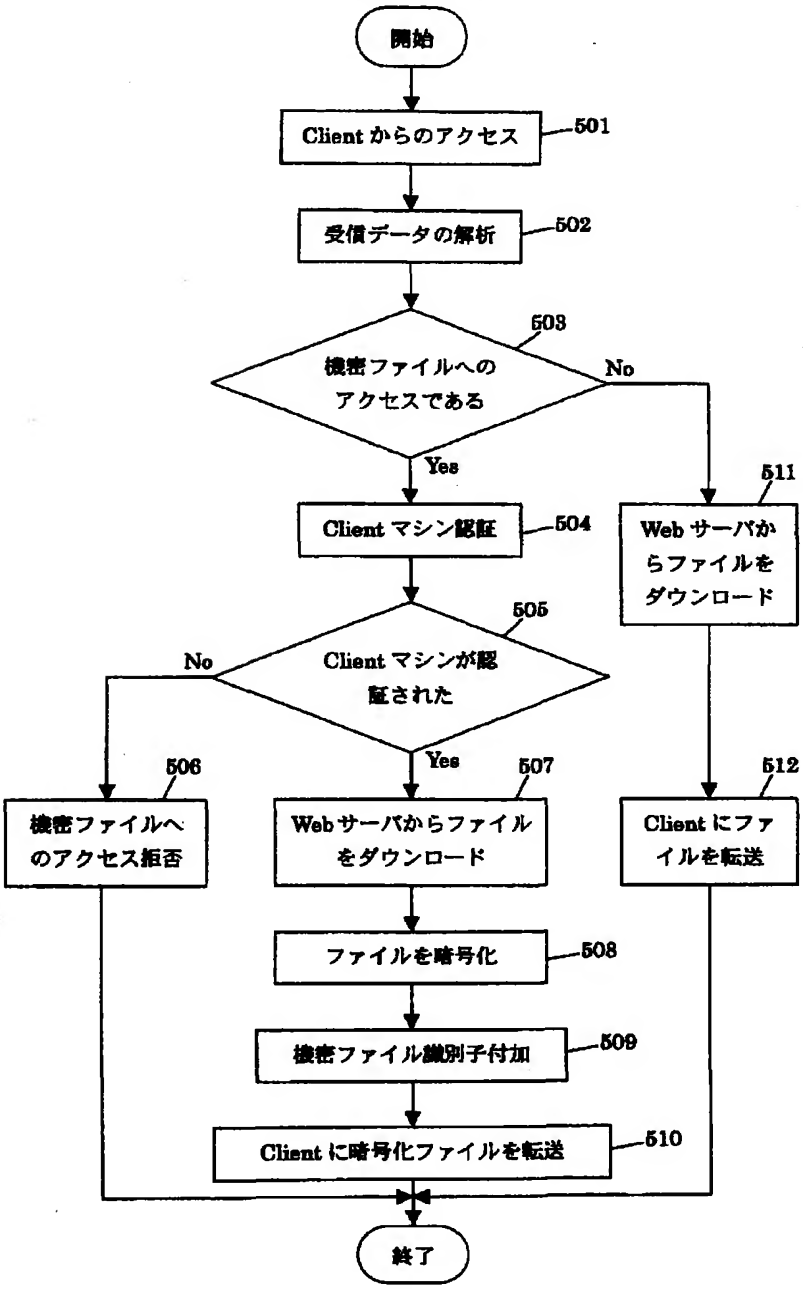
2104 識別番号	2105 ユーザ ID	2106 password
001	user001	＊＊＊＊＊
002	user002	＊＊＊＊＊＊＊＊
003	user003	＊＊＊＊＊＊＊
⋮	⋮	⋮

【図２４】

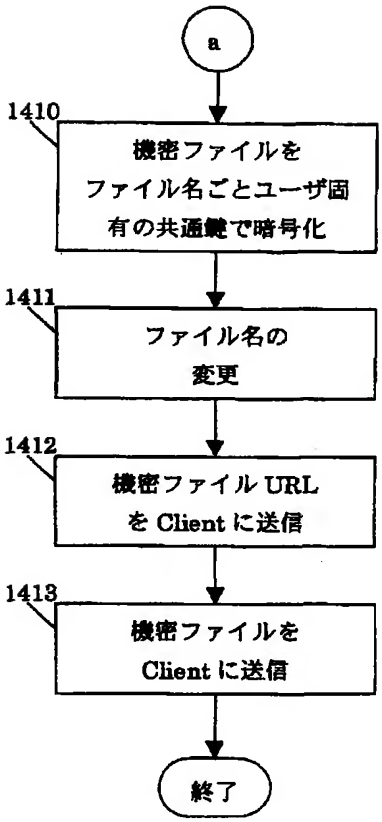


【図５】

Proxy サーバにおける処理のフローチャート

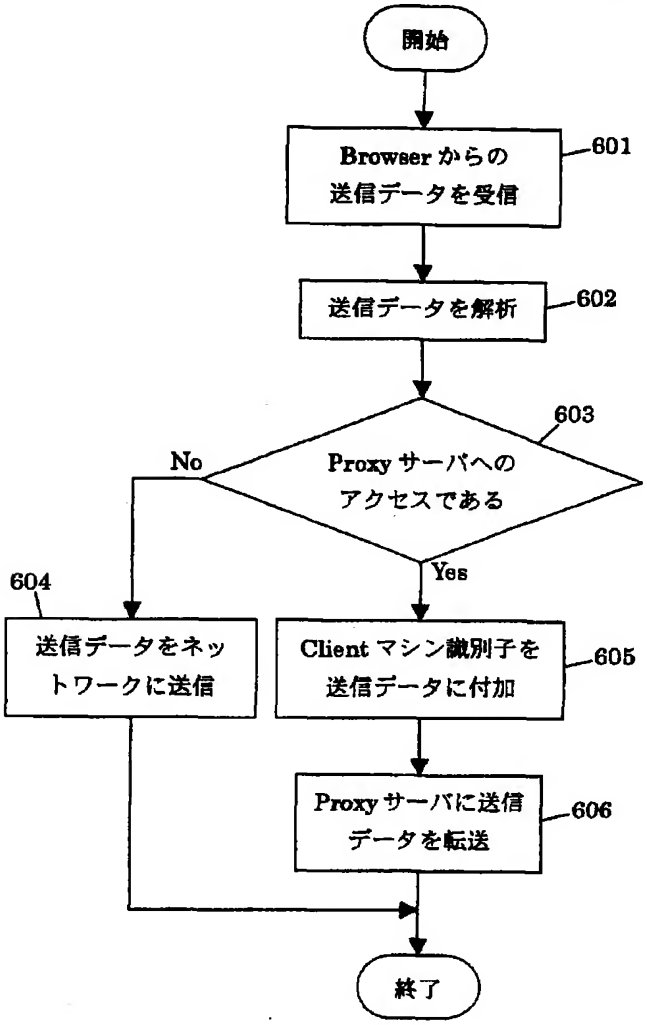


【図１５】

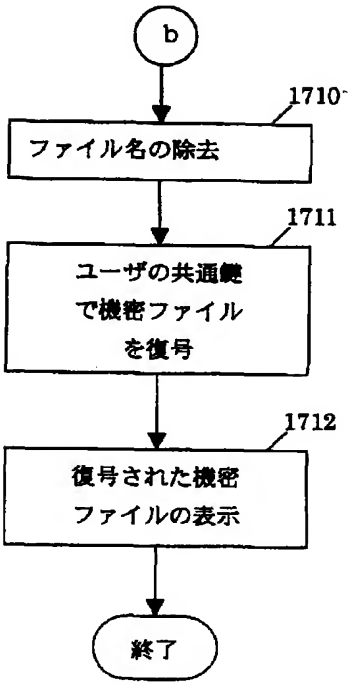


【図６】

通信フックモジュールにおいて、データ送信時における処理のフローチャート

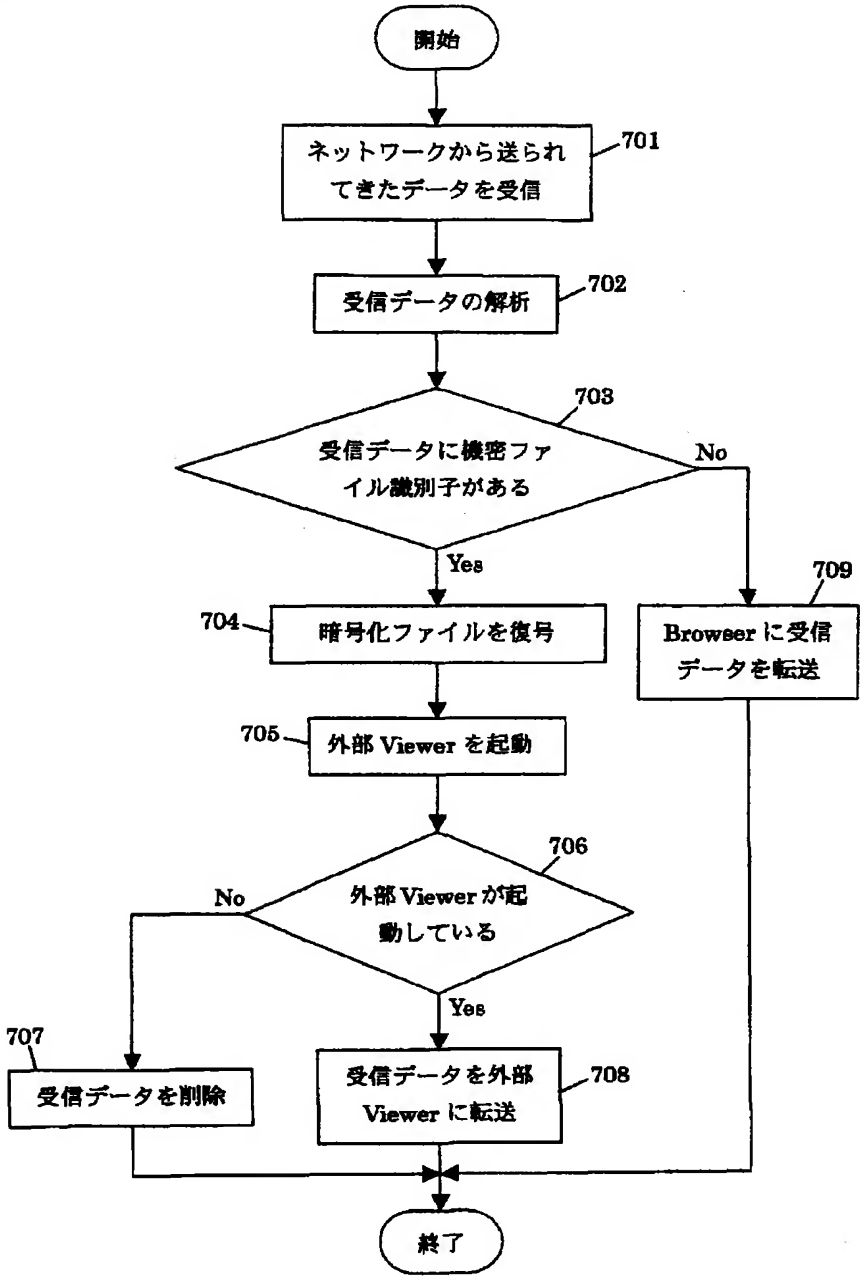


【図１８】



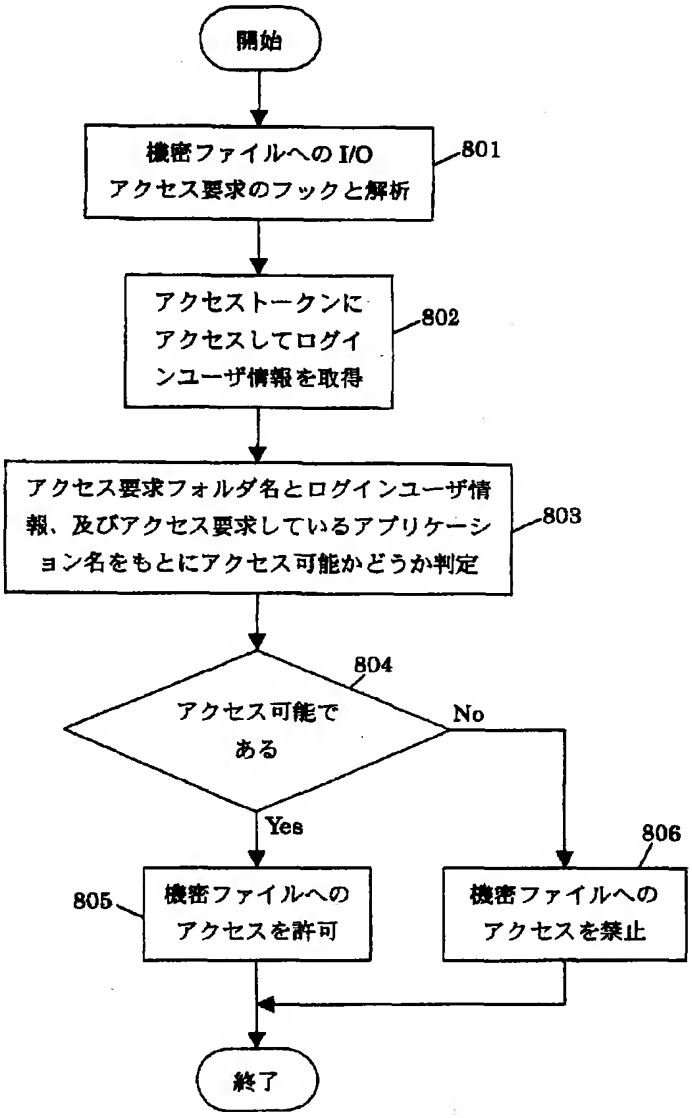
【図７】

通信フックモジュールにおいて、データ受信時における処理のフローチャート



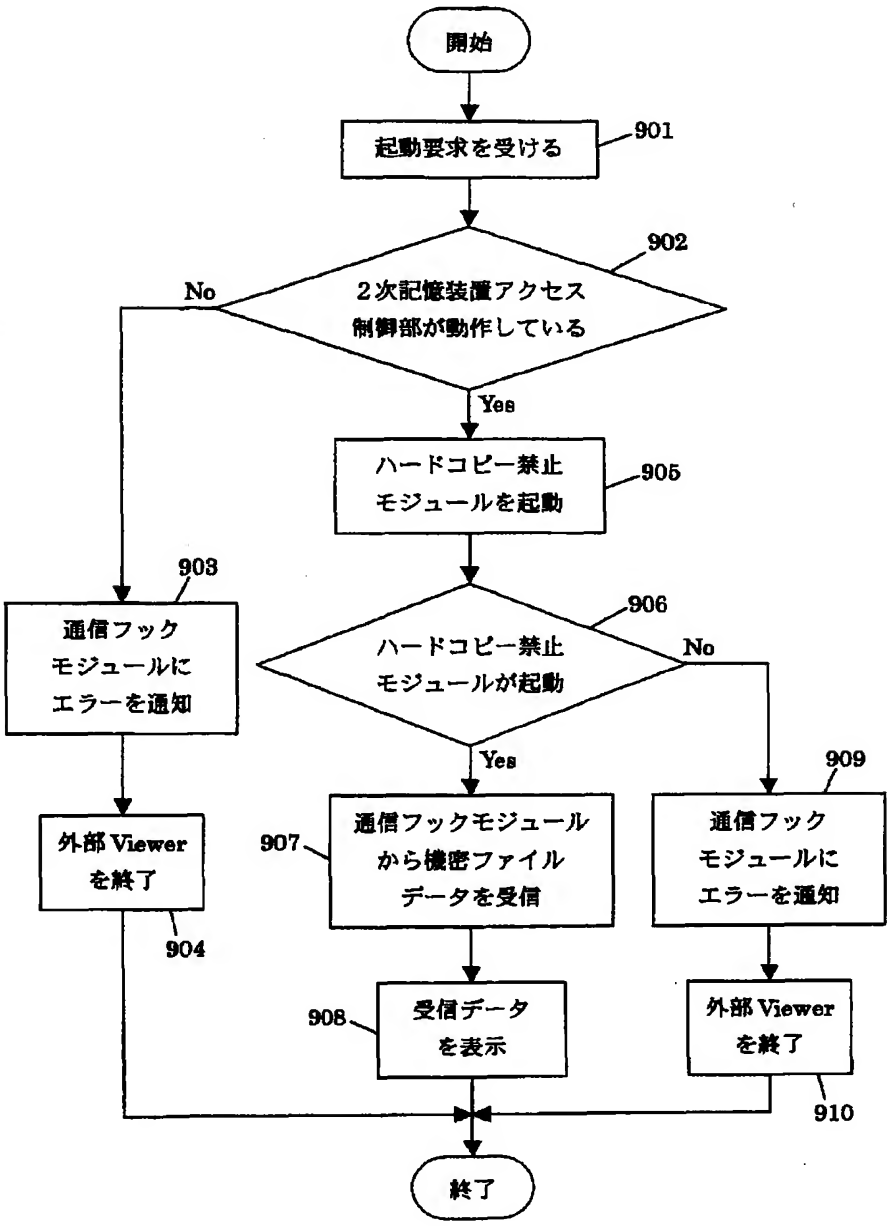
【図８】

２次記憶装置アクセス制御部おける機密ファイルアクセス時の処理のフローチャート

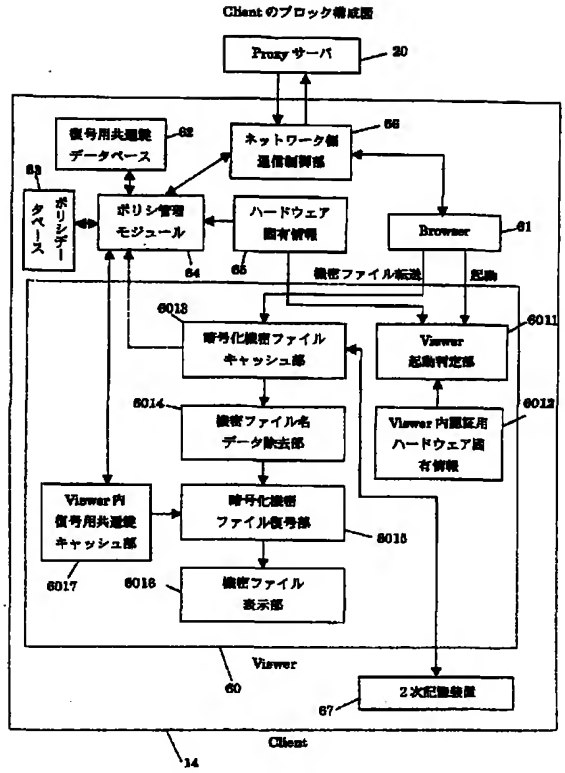


【図９】

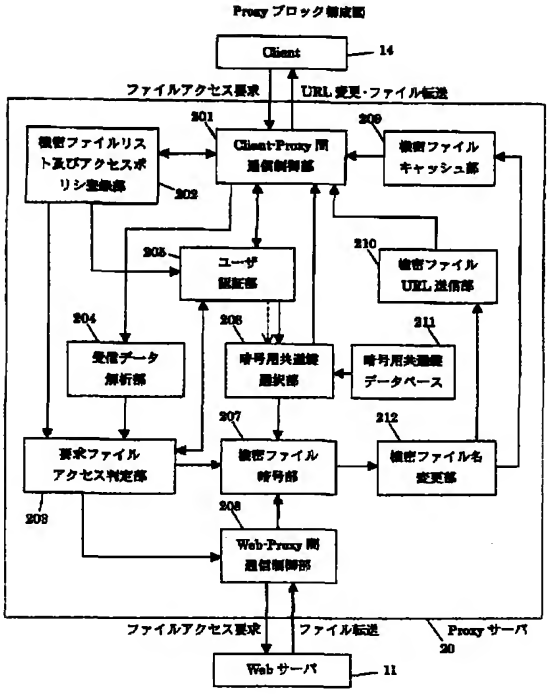
外部 Viewer における受信データ表示処理のフローチャート



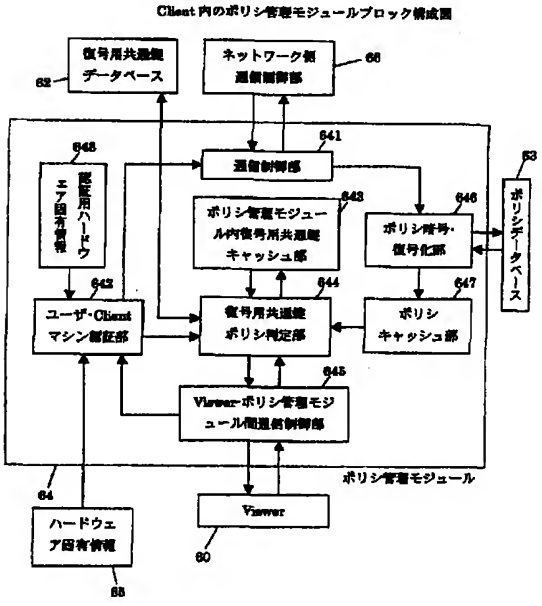
【図１１】



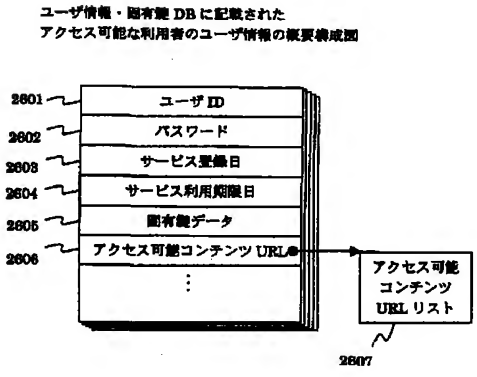
【図１２】



【図１３】

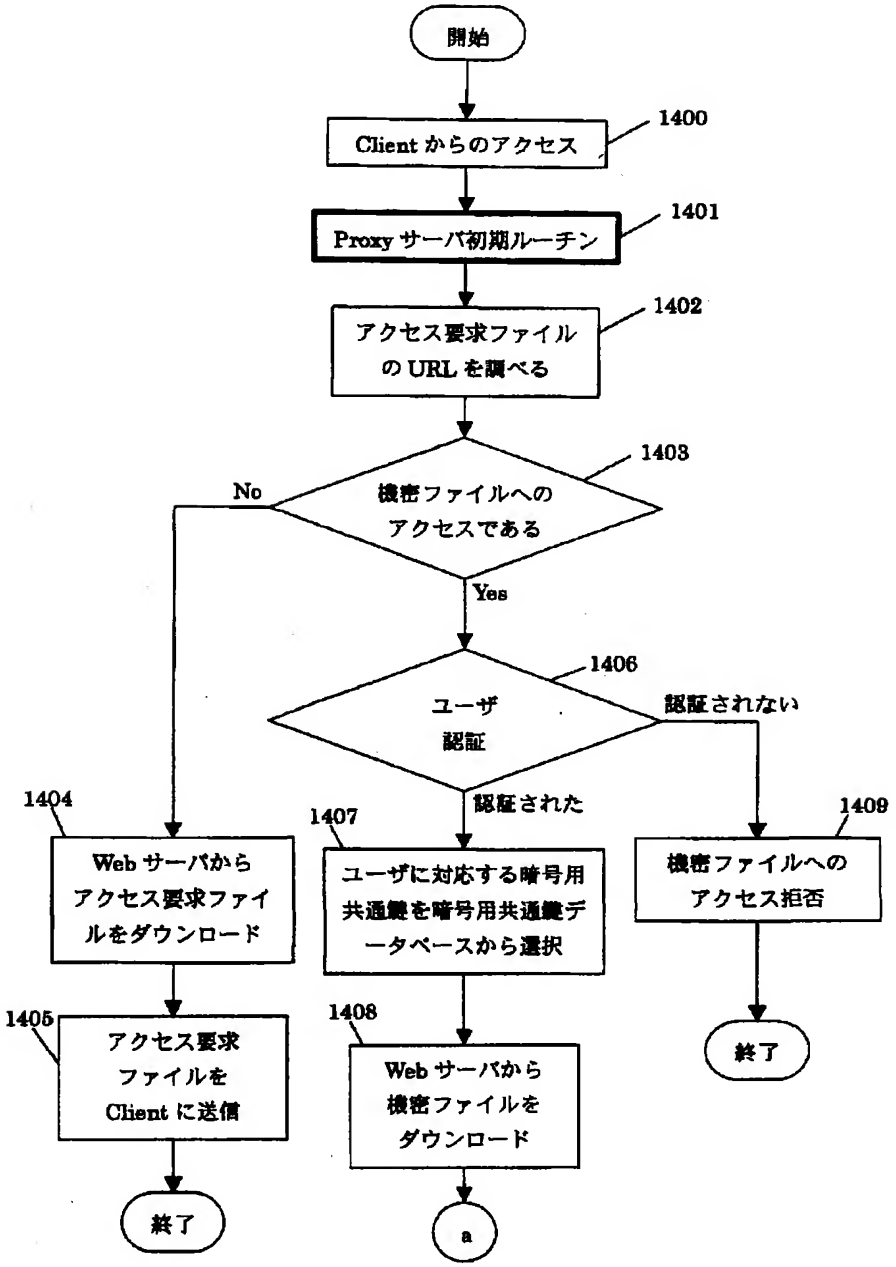


【図２６】



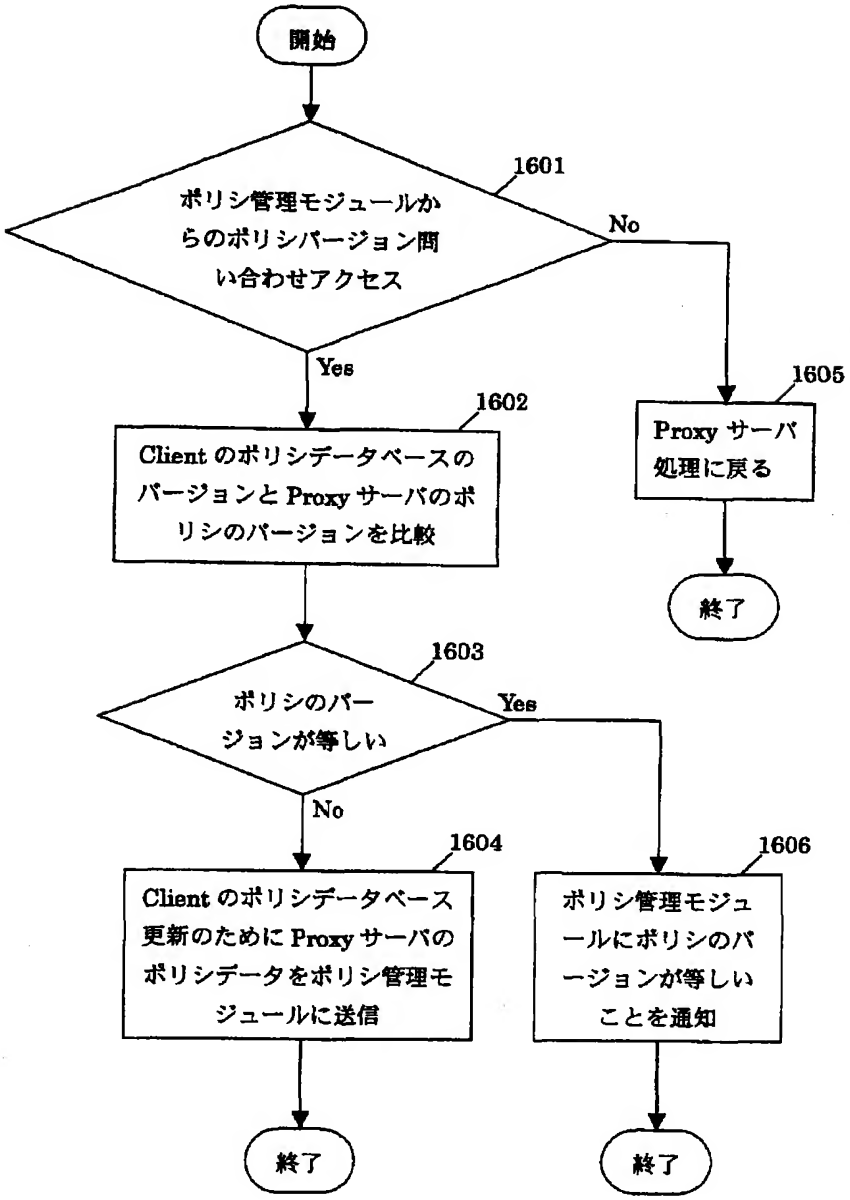
【図１４】

Proxy サーバにおける処理のフローチャート



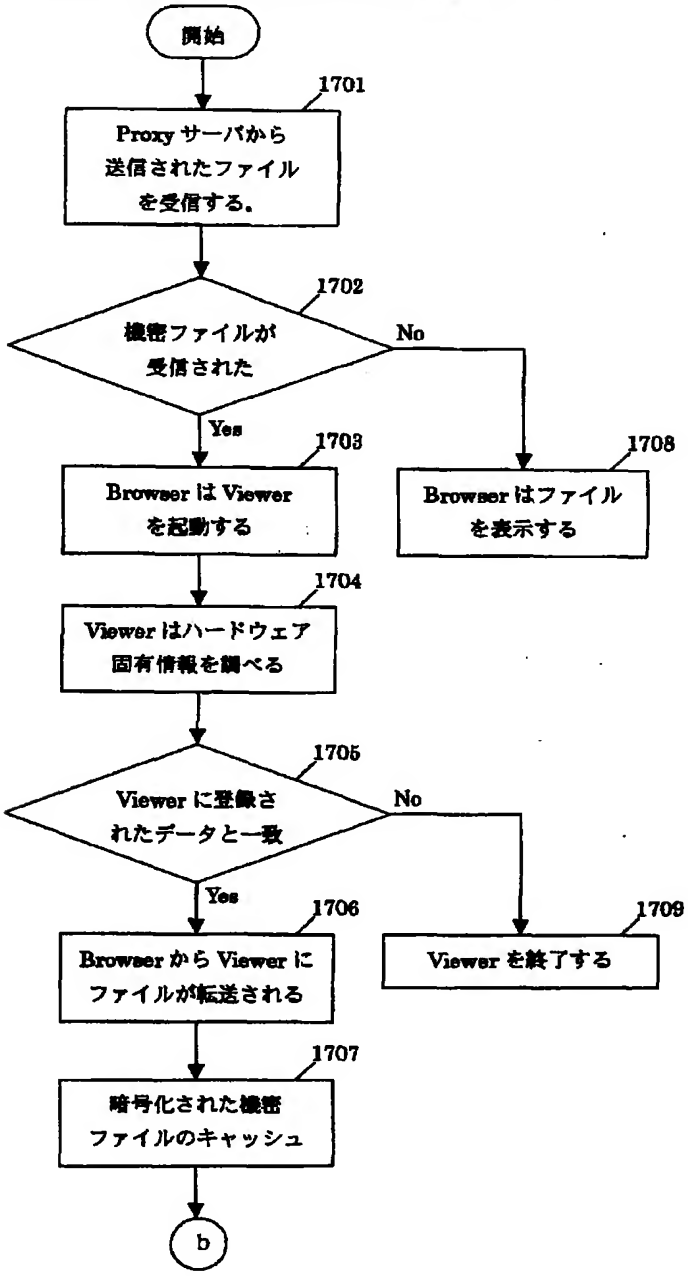
【図１６】

Proxy サーバ初期ルーチンフローチャート



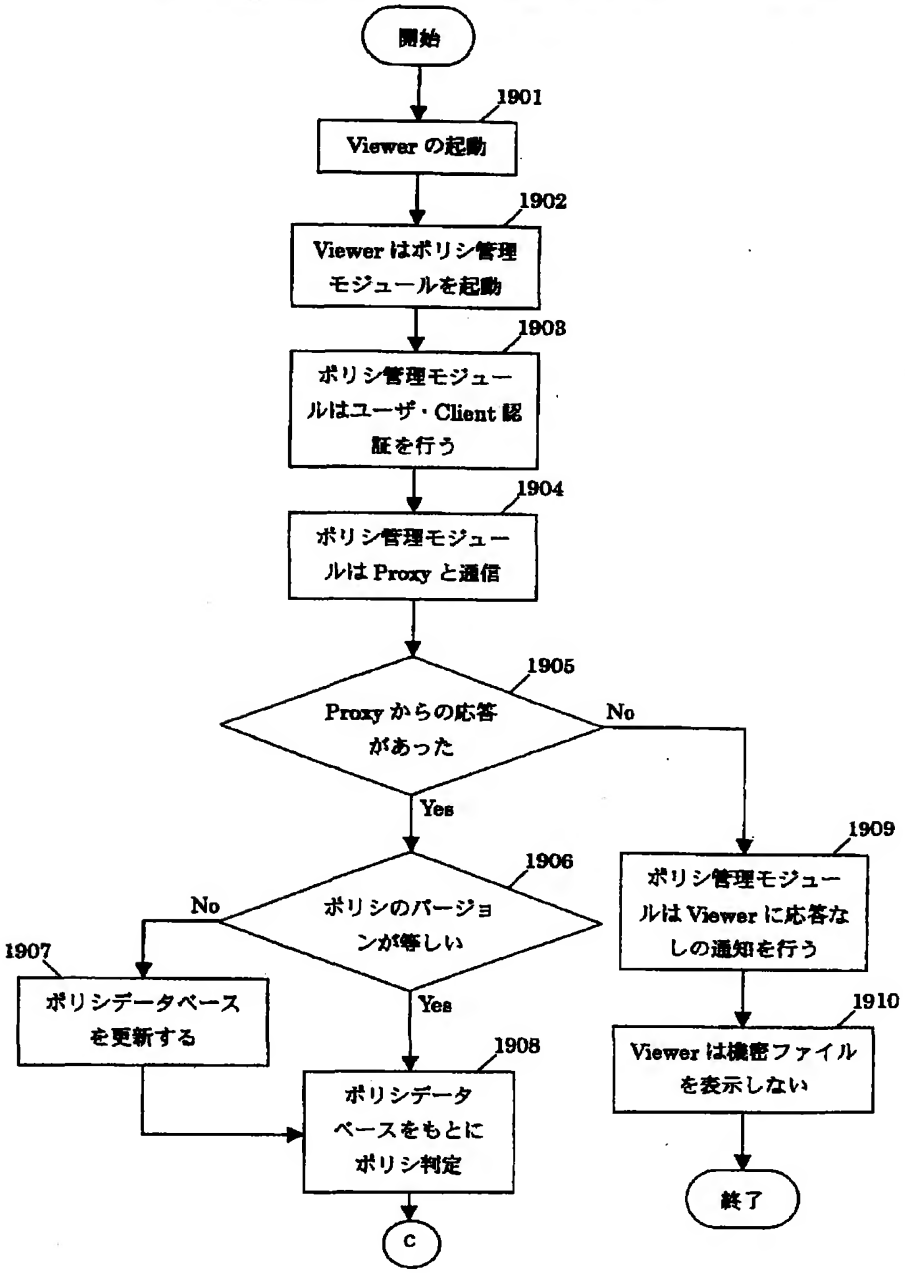
【図１７】

Web サーバ上のファイル参照時の Client における処理のフローチャート

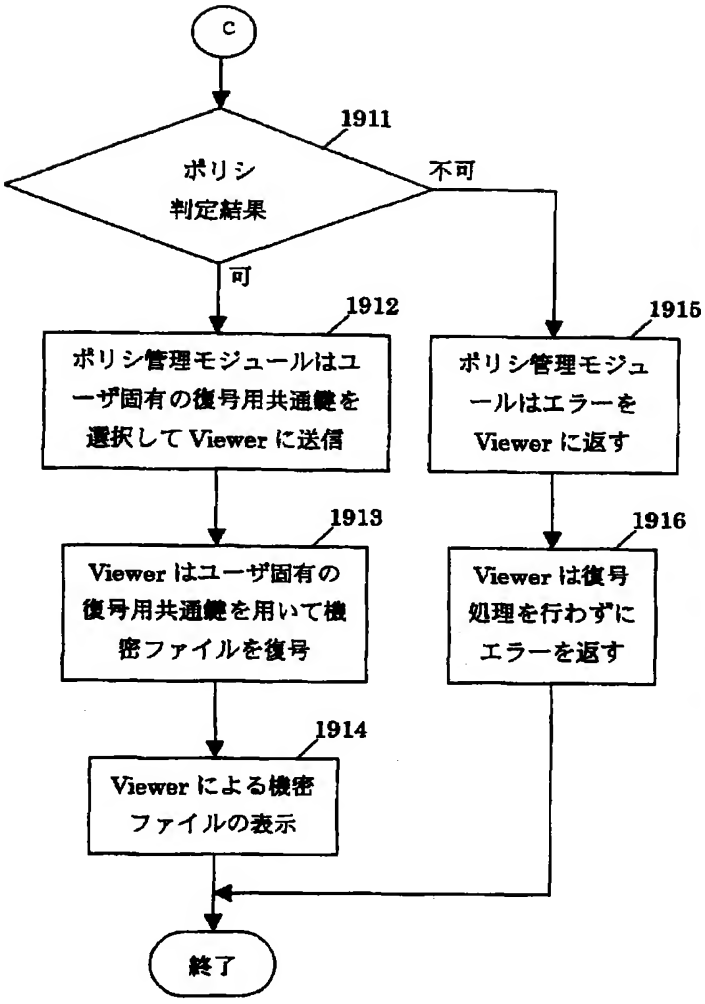


【図１９】

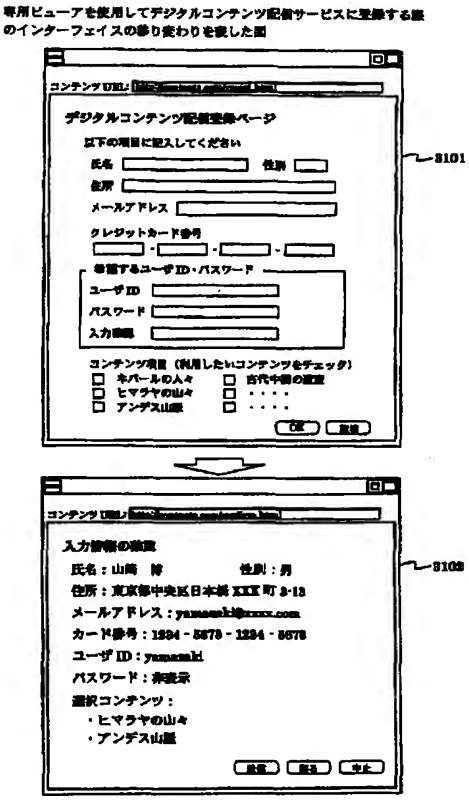
２次記憶装置に保存された機密ファイル参照時の Client における処理



【図２０】

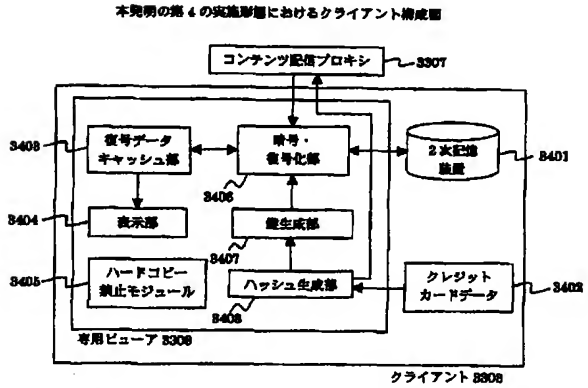


【図３１】

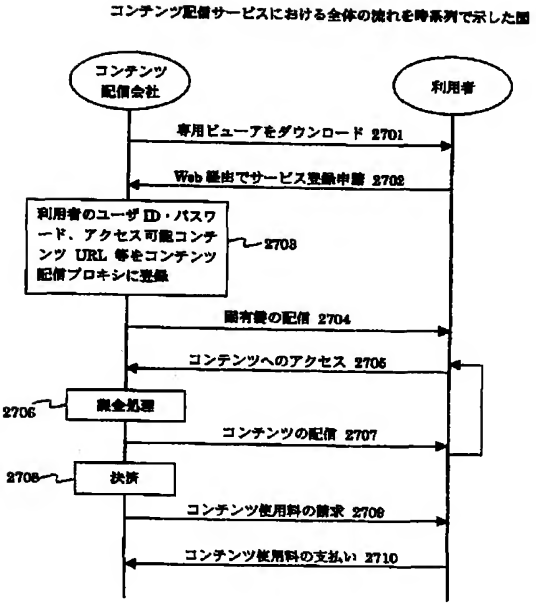


【図３２】

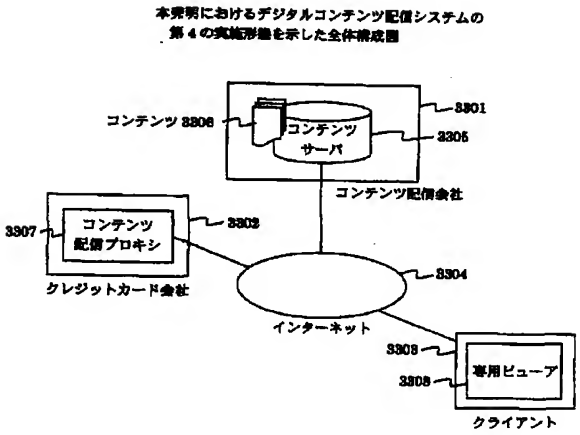
【図３４】



【図２７】

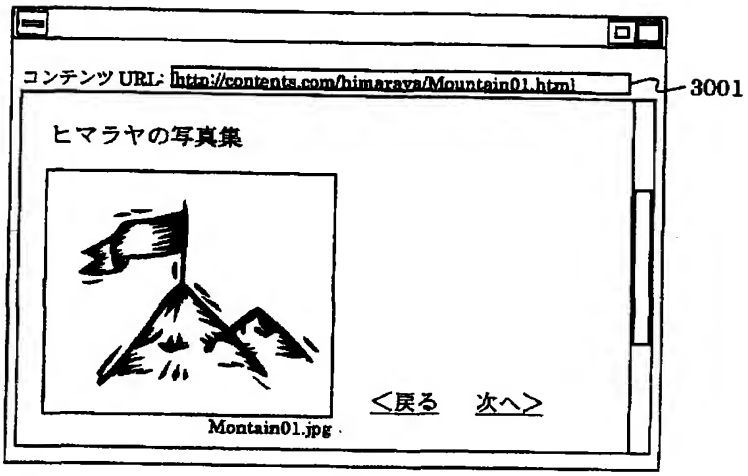


【図３３】



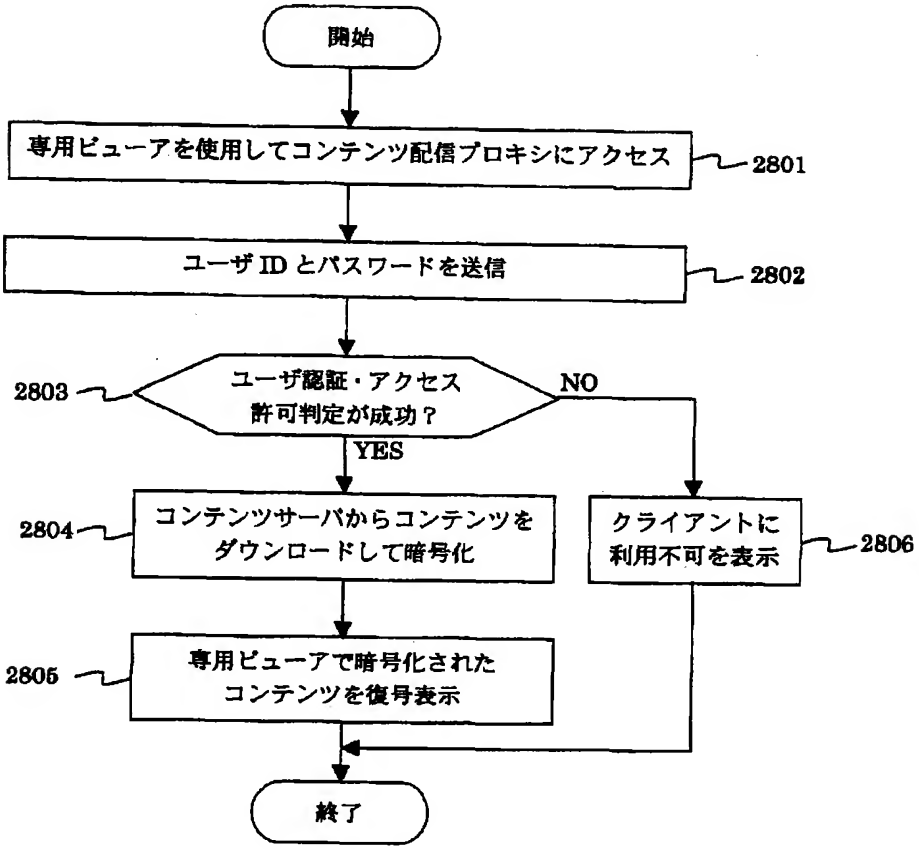
【図３０】

専用ビューアインターフェイス図

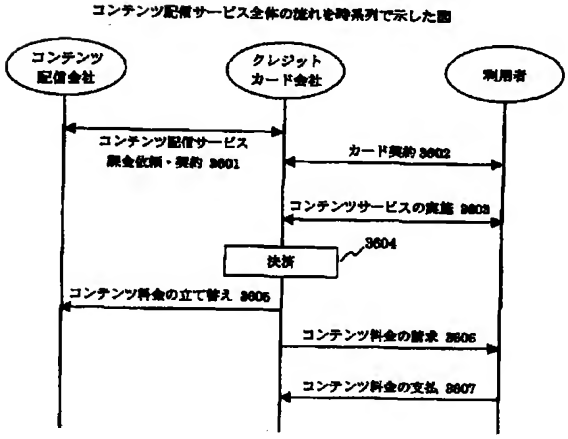


【図２８】

コンテンツをダウンロードして専用ビューアで閲覧する際のフローチャート

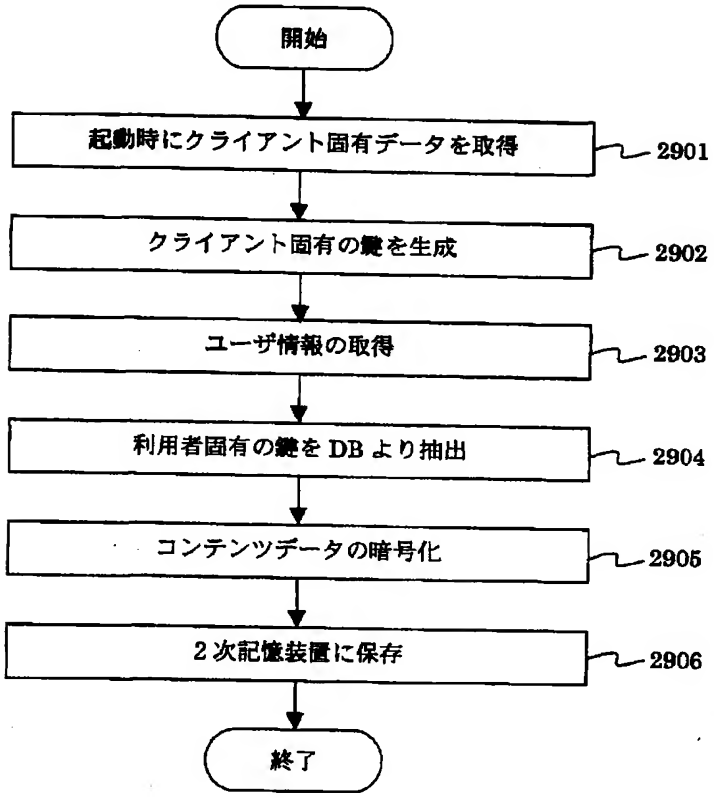


【図３６】

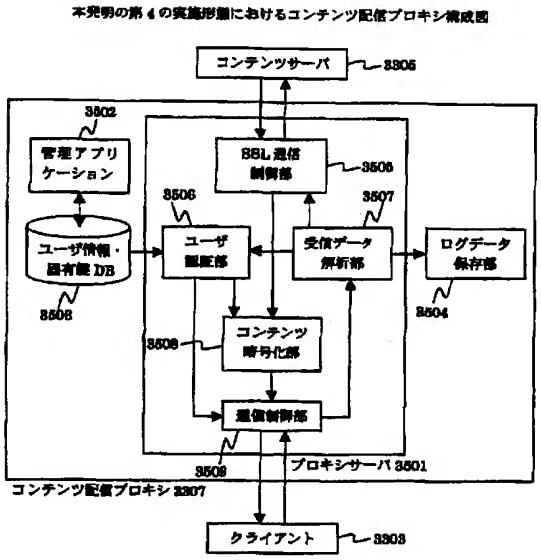


【図２９】

クライアントにコンテンツデータを保存する際の
専用ビューアが行う処理のフローチャート

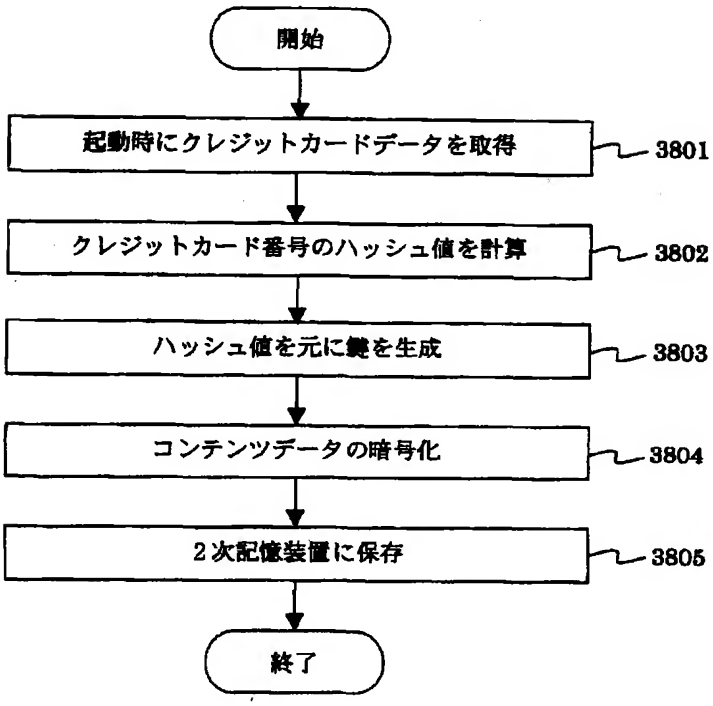


【図３５】



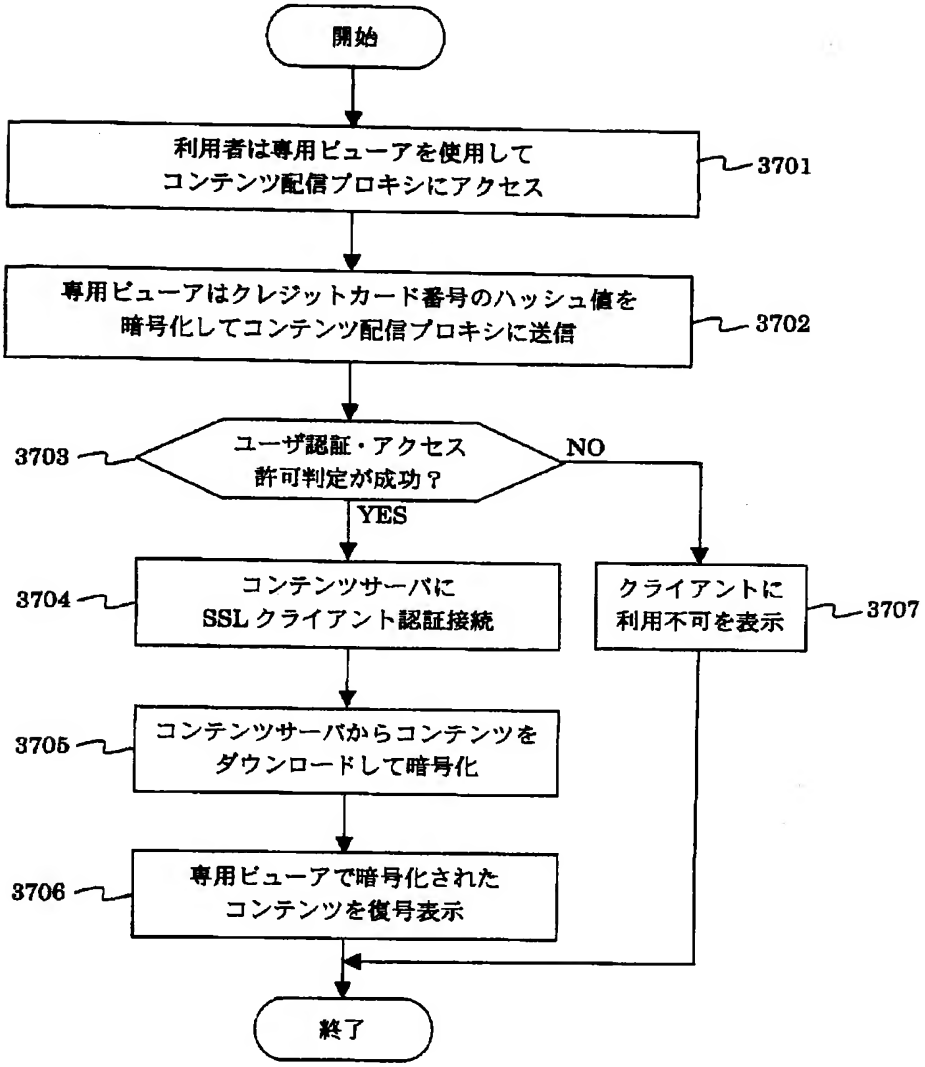
【図３８】

クライアントにコンテンツデータを保存する際の専用ビューアが行う処理のフローチャート

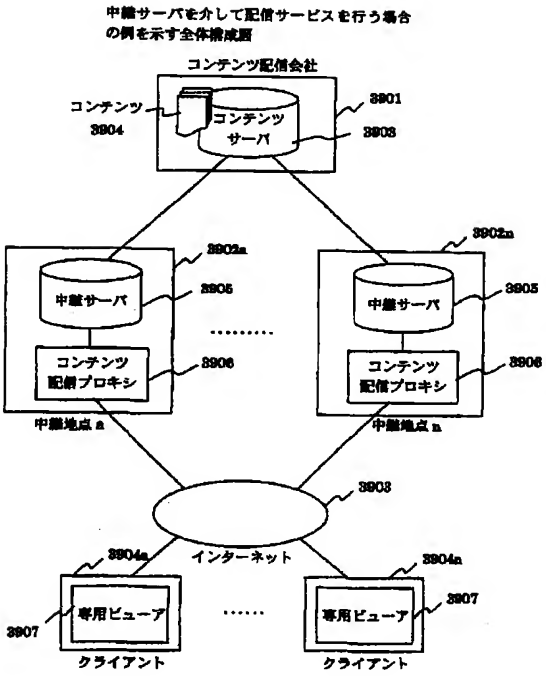


【図３７】

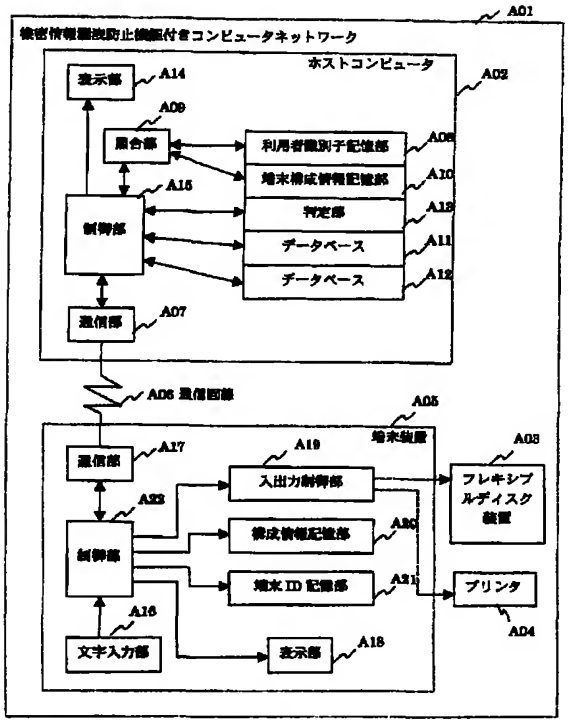
コンテンツをダウンロードして専用ビューアで閲覧する際のシステム全体のフローチャート



【図３９】


中継サーバを介して配信サービスを行う場合の例を示す全体構成図
コンテンツ配信会社
コンテンツ
3904
コンテンツサーバ
3901
3902
3902a
中継サーバ
3905
コンテンツ配信プロキシ
3906
中継地点 a
3902n
中継サーバ
3905
コンテンツ配信プロキシ
3906
中継地点 n
3903
インターネット
3904a
専用ビューア
3907
クライアント
3904n
専用ビューア
3907
クライアント

【図４０】


A01
機密情報漏洩防止機能付きコンピュータネットワーク
ホストコンピュータ
A02
表示部
A14
A09
照合部
利用者識別子記憶部
A08
端末構成情報記憶部
A10
制御部
A15
判定部
A13
データベース
A11
データベース
A12
通信部
A07
A06 通信回線
A05
端末装置
通信部
A17
A19
入出力制御部
A03
フレキシブルディスク装置
A23
制御部
構成情報記憶部
A20
端末 ID 記憶部
A21
プリンタ
A04
A16
文字入力部
表示部
A18